Avaya VoIP Monitoring Manager Reference

14-300614
Issue 2
February 2006

Table Of Contents

About VoIP Monitoring Manager 1
Search for Endpoints 1
View Reports 1
Export Reports 1
Generate Automatic Alarms 1
About VoIP Monitoring Manager Client 2
About VoIP Monitoring Manager Web Client 2
About VoIP Monitoring Manager Server 2
Components of VoIP Monitoring Manager 2
About Licenses 3
Help 4
What's this help 4
Context-sensitive help 4
About menu 4
Send us feedback! 4
Support Details 4
Installation Checklist 5
Installation Checklist 5
Configure IP-Network-Region form 6
Configure System-Parameters IP-Options Form 7
Make one port available 7
Check Windows SNMP Agent is Installed and Running 7
Check for a Valid SNMP Community ID 8
Configure SNMP Service For Sending Traps 9
Connect to Database 10
Manage your licenses 10
Customized Setup 11
Change Monitoring Manager Server 11
Configure Database Tables 11
Migrate Data 11
Overview of VoIP Monitoring Manager Client 13
VoIP Monitoring Manager Client 13
System Pane 13
Endpoints Pane 14
Connection Status 16

Status Bar 16
Search Dialog Box 16
Results List 17
View Tool Bar 19
Search Button 19
Getting Started Guide (Client) 20
Starting VoIP Monitoring Manager Client 20
How to Use VoIP Monitoring Manager Client 20
Starting VoIP Monitoring Manager Web Client 20
Run a Search 21
View a Report 22
How to... (Client) 23
Connect to New Server 23
Run a Search 23
Search Dialog Box 24
Advanced Search 24
Search for a Specific Network Address 25
Search for a Specific Phone Number 26
Search for a Specific SIP Username 26
Search Using Quality of Service (QoS) Values 27
View Results List 27
Export Result List 27
Creating Reports with Exported Data 28
View Active Endpoints 28
View Status Bar 28
Update System View 28
Configure Friendly Names for Gateways 28
About Dialog 30
Working with Reports (Client) 31
About Summary Reports 31
About Detailed Reports 32
About Session Properties 34
Difference Between Endpoint and Session Reports 35
Summary Session Report 35
Detailed Reports for Endpoints 38
Summary Media Gateway Link Report 39
Detailed Media Gateway Link Report 41

Trace Routes Media Gateway Link Report 43
View a Report 43
Close Report 44
Close All Reports 44
Copy Report 44
Move the Reports 44
Update Report 45
Update All Reports 45
Edit Report Properties 45
Changing the Date Range of Reports 46
Interpreting Reports 47
Interpreting the Values Using Summary Reports 47
Arranging Reports 49
Export Data (Client) 51
Export Result List 51
Export Report Data (one session) 52
Creating Reports with Exported Data 52
Overview of VoIP Monitoring Manager (Server) 53
VoIP Monitoring Manager Options 53
About RTCP Monitor 56
Components of RTT 57
Activity Monitor 57
About the Database 57
Data Storage Limits and Management 57
Storage Options 58
License Server Administration Dialog Box 58
About Dialog 59
Getting Started with VoIP Monitoring Manager (Server) 60
Starting VoIP Monitoring Manager Client 60
Starting VoIP Monitoring Manager Web Client 60
Monitoring Server Status 61
Connect to RTCP Monitor 62
Changing the RTCP Listen Port 62
Connecting to the License Server 62
Generating Traps & Alarms (Server) 63
Generating Traps and Alarms 63
Recommended Trap Settings 63

Call Traps 64
System Traps 65
Terminal Traps 66
Troubleshooting 67
Troubleshooting 67
License Problems 67
Client Error Messages 67
Client Error Messages 67
Access Error 67
Graph Limit Reached 67
Help Could Not Be Displayed 67
Invalid Bounds 68
Invalid Date Range 68
Invalid Search Parameter 68
No Data is Displaying on a Report 68
No Endpoint Data Available 68
No Endpoints Matched the Search 69
Server Unavailable 69
Server Version Error 70
Some Fields Are Blank in the Exported Data 70
Unknown Error 70
Web Client Displaying Incorrect Time 71
Windows SNMP Agent Connection Error 71
Server Error Messages 71
Server Error Messages 71
Check SNMP Installation 71
Could Not Resolve Host Name 71
Excessive Packet Loss 71
General Server Error 72
Invalid RTCP Port 72
Ports used by Server 72
Problems Binding to Port 162 72
RMI Registry Error 73
Set RTCP Port Error 73
Server Cannot Connect to SNMP 73
SNMP Service Error 74

Unable to establish database connection 74
Windows SNMP Agent is Not Running 74
Reference Information 75
Characteristics of RTCP 75
Database Schema 75
Entity Relationship Diagram 80
Handling Jitter 81
Interpreting RSVP Status 81
Interpreting Terminal Names 82
SNMP Community ID 82
TTL Considerations 83
Glossary 84
Index 91

About VoIP Monitoring Manager

Avaya VoIP Monitoring Manager is a Voice over IP (VoIP) Quality of Service (QoS) monitoring tool. It enables you to monitor and review the quality of a call on an Avaya VoIP network. Avaya VoIP Monitoring Manager allows you to view the QoS data (such as Jitter, Round Trip Time (RTT) and Packet Loss) experienced at the endpoints and during a session. The QoS data displays in real-time or for previously active endpoints. With this information, you can begin to troubleshoot and isolate problems.

If you are new to using the VoIP Monitoring Manager, the following information explains what you can do with this tool.

Search for Endpoints

You can search endpoints active from a specified time in the past or within a date range. The Advanced Search options enable you to narrow your search to match phone numbers, SIP user names, network addresses, or QoS level.

View Reports

Once you have completed your search, you can select one or more endpoints in a session and view the associated reports. The reports display the QoS data for the selected endpoints. This is particularly useful for monitoring media gateways or locating problems at a particular endpoint.

Since you can view reports for endpoints involved in a session, this information will assist you with determining problems that occur between two endpoints or in an isolated area of the network.

Export Reports

You can export the report data to a comma separated value (csv) file. You can open this file in most database and spreadsheet programs such as Microsoft Excel. Exporting the data to a spreadsheet enables you to manipulate the data so you can create your own reports..

Generate Automatic Alarms

You can generate Simple Network Management Protocol (SNMP) traps/alarms, which allow the VoIP Monitoring Manager to alert you when the Jitter, Round Trip Time or packet loss reaches certain levels. This assists you to routinely monitor the network and troubleshoot problems.

About VoIP Monitoring Manager Client

The VoIP Monitoring Manager (VMM) Client provides the graphical user interface (GUI) to view the VMM data. The VMM Client does not communicate with the VMM RTCP Monitor, does not use SNMP, and does not communicate with the database. The data that is displayed is gathered from the VoIP Monitoring Manager (VMM) Server.

The VMM Client may be installed on the same machine as the VMM Server, or it may be installed on another PC on the network. It is possible for the VMM Server and the VMM Client to communicate over a dial-up connection.

About VoIP Monitoring Manager Web Client

The VoIP Monitoring Manager (VMM) Client can run as a web application in a browser. This is useful if you only have the VMM Server installed. To run the VMM Client as a web application, the following requirements must be met:

- The VMM Server needs to be running a web server. The Apache web server is automatically installed on the server when the VMM Server software is installed.
- The web server must be configured to publish the file to the following VMM installation path:
  C:\Program Files\Avaya\VoIP Monitoring Manager\jars\ClientApplet.htm

  NOTE:
  The server installation will apply this configuration.
- The PC you will use to access the VMM Server must be able to connect to the VMM Server via a web browser and have the following software installed:
  - Microsoft Internet Explorer 6.0 or later
  - Sun Java 2 Runtime Environment, SE v1.4.2_06.

If you run the web client, you will not have access to all the functionality available in the VMM Client application. For example, you will be unable to copy and connect to a new server. For more information, see Starting VoIP Monitoring Manager Web Client.

About VoIP Monitoring Manager Server

The VoIP Monitoring Manager Server acts as a proxy between the database and the VoIP Monitoring Manager Client. It manages connectivity to the database and provides an interface to configure the VoIP Monitoring Manager RTCP Monitor. The main purpose of the VoIP Monitoring Manager Server is to reduce the amount of traffic to the VoIP Monitoring Manager Client by performing large data downloads and extensive processing of the MIB data stored on the RTCP Monitor.

The VoIP Monitoring Manager Server is a Java application that runs as a Windows service on the same PC as the RTCP Monitor. The VoIP Monitoring Manager Server can reside on the same PC as the RTCP Monitor, or it can reside on a separate PC.

Components of VoIP Monitoring Manager

The VoIP Monitoring Manager (VMM) application consists of the VMM RTCP Monitor and the VMM Server, which accepts connections from the VMM Client. If you only have the VMM Server installed, you can run VMM Client as a web client.

To ensure VMM will run correctly, you must perform the following steps:

- Configure the Switch Administration Forms on Avaya Communication Manager.
- Install a Windows SNMP Agent on the server (if not installed already).
- Install the VMM Server on to the network.

The components and their relationship are described in more detail in the following links:

- VoIP Monitoring Manager Server
- VoIP Monitoring Manager RTCP Monitor
- VoIP Monitoring Manager Client
- VoIP Monitoring Manager Web Client
- Database

About Licenses

VoIP Monitoring Manager requires licenses that you must purchase from Avaya. You can purchase these licenses in sets of 2000 phone endpoints and 40 media gateways. The Avaya licenses are managed by the WebLM server, which is provided with VoIP Monitoring Manager.

By selecting **Help>About** in the VMM Server window or the VMM Client, you can view the following information:

- the number of licenses purchased
- the number of phones at the local server. This number represents the phones that reported to VMM in the last 28 days. This number will increase if you move phones (for example, change extensions or IP addresses). In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, this will not be a problem.
- the number of phones at the local server that exceed the license (that is, the number of phones that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more phones stored in the database than licenses purchased.
- the number of media gateways at the local server. This number represents the media gateways that reported to VMM in the last 28 days.
- the number of media gateways at the local server that exceed the license (that is, the number of media gateways that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more media gateways stored in the database than licenses purchased.

Each VMM RTCP monitor periodically checks the number of endpoints it knows about and requests/renews the licenses for them. If there is more than one RTCP monitor and the total number of endpoints known exceeds the number of licenses, the RTCP monitor that requests licenses first will get its licenses. The RTCP monitor that requests licenses last will be denied licenses. If you enter the 30-day grace period because license limits were exceeded, the About dialog box will appear every time you start the VMM Client or open the VMM Server window. If you exceed the 30-day grace period, VoIP Monitoring Manager Server stops collecting RTCP data.

Avaya provides a 90-day trial version of VoIP Monitoring Manager. After 90 days, VoIP Monitoring Manager stops collecting RTCP data. You have the option of purchasing the VoIP Monitoring Manager license key from Avaya to fully activate the VoIP Monitoring Manager beyond the 90-day trial period. When a license key is purchased, an instance of WebLM License Server is required to manage the license key.

Contact your authorized Avaya Sales Representative to purchase additional VMM licenses.

Help

Most screens and tasks in VoIP Monitoring Manager have matching topics in this help. You can go directly to the matching topic by clicking the Help button shown on the screen or dialog box.

If the topic displayed does not show the required information, you can open the entire help at any time.

To open the Help Contents, select **Help** > **Contents**.

To open the Help File, click on this icon on the **Tool Bar** or **Help** > **Contents**.

What's this help

The What's this? button located on the Tool Bar enables you find out what a **Tool Bar** or button is in the application. You click on the **What's this?** button as shown above and then click the object. The help will open explaining that particular object.

Context-sensitive help

If you click the help button on a form, help about that form (or its uses) is displayed.

About menu

You access the About menu from **Help > About**. The About dialog box shows the version number for the VoIP Monitoring Manager (VMM) Client. This is useful to ensure that you are using the same version number for the VMM Client as the VMM Server.

Send us feedback!

To send us feedback or to suggest any improvements about this Online Help, send an email to performance@avaya.com.

Support Details

If you require further support details for VoIP Monitoring Manager, check the Avaya web site located at www.avaya.com for the most recent information. From the main page, navigate to the support page, and search for VoIP Monitoring Manager.

Installation Checklist

Installation Checklist

The VoIP Monitoring Manager Server (VMM Server) needs to be installed on the VoIP network. Before you install the software, you need to configure the Switch Administration Forms on Avaya Communication Manager.

1. Configure Switch Administrator forms.

   You need to configure the System-Parameters IP-Options Form and the IP-Network-Region Form to send RTCP reports to the RTCP Monitor.

2. Make one port 1099.

   The VMM Client and Server communicate using Java Remote Method Invocation (RMI), and uses port 1099 as its default port on the machine running the VMM server. If port 1099 is not available, another port must be made available.

3. Check for Windows SNMP Agent.

   The SNMP Agent must be installed for the VoIP Monitoring Manager Server to function. You can check if the Windows SNMP Agent has been configured to run at startup automatically. The installation also checks to see if the Windows SNMP Agent is installed.

   If the Windows SNMP Agent is not installed, the **Add/Remove Windows Components** starts automatically and you are be prompted for the Windows 2000 CD location to install the Windows SNMP Agent.

4. Check for a valid SNMP Community ID.

   You must set an ID with the correct privileges.

5. Configure SNMP agent for sending traps.

   Although SNMP is installed and running, it does not send the required traps until you configure it.

6. Install VoIP Monitoring Manager.

   Insert the CD into your drive and follow the instructions.

7. Connect to a database.

   When you first install VoIP Monitoring Manager, you need to connect the VMM Server to a database.

Solving Installations Problems: If you are experiencing difficulties running the application after installation, the following checks may assist you:

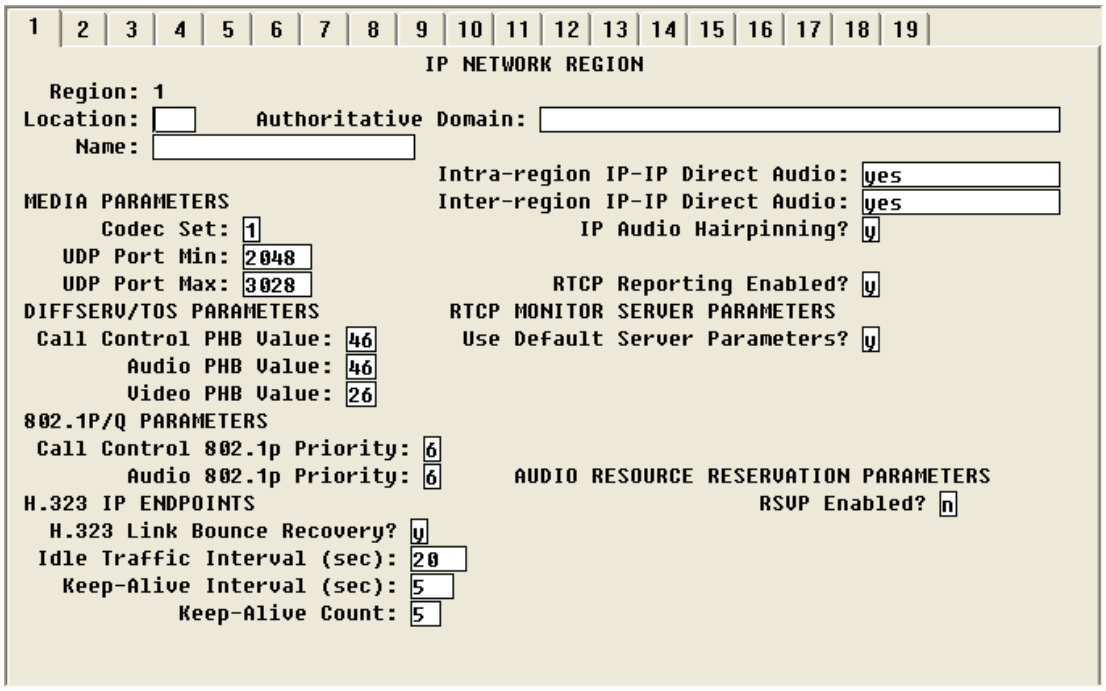
- Check Windows SNMP Agent is Running
- Check for a Valid Community ID

Configure IP-Network-Region form

You must configure two Switch Administration Forms (SAT) on Avaya Communication Manager to send RTCP reports to the RTCP Monitor. These forms are called the ip-network-region form and the system-parameters ip-options form.

Configuration for the ip-network-region form

- Set the **RTCP Reporting Enabled?** field to **y** (yes).
- Set **Use Default Server Parameters?** field to **y** (yes). This indicates that this network region uses the default values specified previously on the system-parameters-ip-options form as well.


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
IP NETWORK REGION
Region: 1
Location: Authoritative Domain:
Name:
Intra-region IP-IP Direct Audio: yes
MEDIA PARAMETERS
Inter-region IP-IP Direct Audio: yes
Codec Set: 1
IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3028
RTCP Reporting Enabled? y
DIFFSERV/TOS PARAMETERS
RTCP MONITOR SERVER PARAMETERS
Call Control PHB Value: 46
Use Default Server Parameters? y
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5

Why you might not want to use the default parameters?

Multiple VoIP Monitoring Manager Servers might be installed on a large system in order to reduce the network traffic between a set of endpoints and the RTCP Monitor (for example, low bandwidth link between endpoints in one network region and a remote RTCP Monitor). The network traffic due to RTCP reports being sent from the endpoints to the RTCP Monitor is usually low, less than 40 bytes per second per currently active VoIP call (RTP session). Therefore, it is usually unnecessary to have multiple RTCP Monitors.

If multiple VoIP Monitoring Manager Servers are installed on the system, then the endpoints in each network region can be configured to send their RTCP reports to different RTCP Monitors. To configure the endpoints in each network region to send their RTCP reports to different RTCP Monitors, perform the following steps:

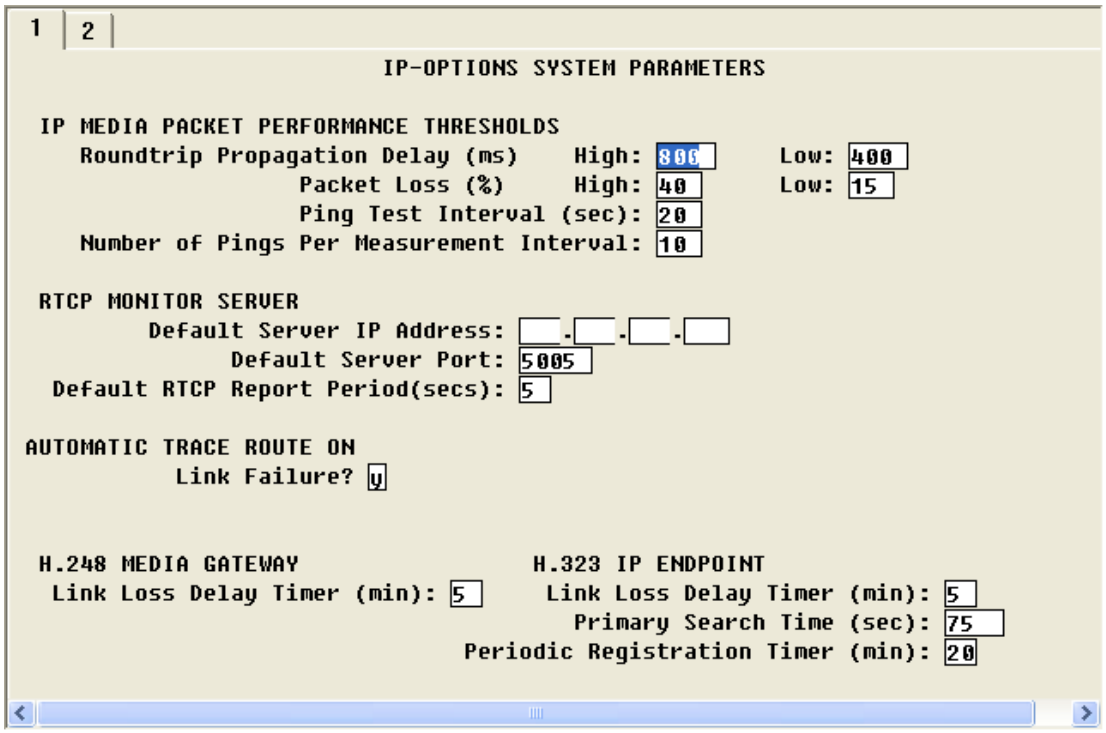
- Set **Use Default Server Parameters?** field to **n** (yes).
- Specify the IP address of the Windows 2000 PC running the VoIP Monitoring Manager Server for that network region.

Configure System-Parameters IP-Options Form

You must configure two Switch Administration Forms (SAT) on Avaya Communication Manager to send RTCP reports to the RTCP Monitor. These forms are called the system-parameters ip-options form and the ip-network-region form.

Configuration for the system-parameters ip-options form

Set the RTCP MONITOR SERVER, Default Server IP Address to the address of the Windows 2000 PC running the VoIP Monitoring Manager Server.


1
2
IP-OPTIONS SYSTEM PARAMETERS
IP MEDIA PACKET PERFORMANCE THRESHOLDS
Roundtrip Propagation Delay (ms) High: 800 Low: 400
Packet Loss (%) High: 40 Low: 15
Ping Test Interval (sec): 20
Number of Pings Per Measurement Interval: 10
RTCP MONITOR SERVER
Default Server IP Address:
Default Server Port: 5005
Default RTCP Report Period(secs): 5
AUTOMATIC TRACE ROUTE ON
Link Failure? y
H.248 MEDIA GATEWAY
Link Loss Delay Timer (min): 5
H.323 IP ENDPOINT
Link Loss Delay Timer (min): 5
Primary Search Time (sec): 75
Periodic Registration Timer (min): 20

Make one port available

The VMM client and server communicate using Java Remote Method Invocation (RMI), and uses the port 1099 on the machine on which the VMM server is running.

If this port is not available, the VMM server will attempt to use the following ports: 49177, 51173, or 63006. Although it is unlikely that all of these ports will be in use on a single machine, please ensure that at least one of these ports is available.

Check Windows SNMP Agent is Installed and Running

The Windows SNMP Agent must be installed before you install the VoIP Monitoring Manager Server. If Windows SNMP Agent is not installed already, you are prompted during the VoIP Monitoring Manager installation to install it from the Windows CD.

NOTE:
If the Windows SNMP Agent is not installed or is not running, you will experience problems receiving data.

Check if Windows SNMP Agent is Installed and Running

1. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down until you see **SNMP Service.** It should have a status as **Started** and Startup Type as **Automatic**. If it is not included in the list, you will need to install it from the Windows CD.
3. If the SNMP Service is listed but not set to run automatically, you will need to change its properties as follows:
    1. Right-click on **SNMP** and select **Properties** from the context menu. The SNMP Service Properties dialog box opens.
    2. Select **Automatic** from the **Startup Type** drop down list.
    3. Click **OK**.

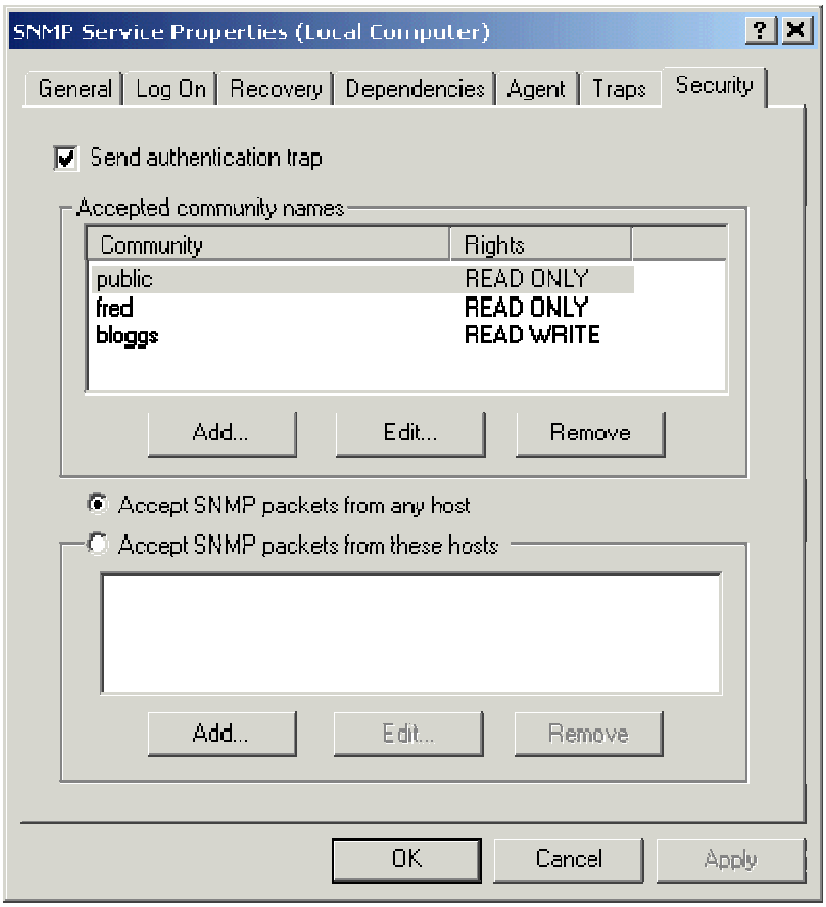
Check for a Valid SNMP Community ID

The Community ID for your Windows SNMP Agent must match the Community ID defined in the VoIP Monitoring Manager Options dialog box. By default it is public, but it may have been changed.

You cannot complete this procedure unless you have already checked that Windows SNMP is installed and running.

To Check for a Valid Community ID

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down and select the **SNMP Service**.
3. Right-click on **SNMP Service**, and select **Properties** from the context menu.
4. Select the **Security** tab. The VoIP Monitoring Manager Options must have a Community ID from the list of Community Names.



5. Add a public ID with Read and Write privileges (if one does not already exist or is not available) for use by VoIP Monitoring Manager.
6. Click **OK**.

Configure SNMP Service For Sending Traps

To send traps, you need to configure the SNMP Service.

To Configure Windows SNMP Agent for Sending Traps

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down and select the **SNMP Service**.
3. Right-click on **SNMP Service**, and select **Properties** from the context menu.
4. Select the **Traps** tab.
5. Type the community name that is configured on the network management system to which trap messages will be sent, and click **Add** to list.
6. In the Trap destinations area, click **Add**. The SNMP Service Configuration dialog box displays.
7. In the **SNMP Service Configuration** dialog box, type the IP address of the network management system to which the traps will be sent, and click **Add**.
8. From the SNMP Service Properties dialog box, click **OK**.

If the changes do not take effect immediately, you may have to restart the SNMP Service. To restart either service, right-click on it, and select **Restart** from the context menu.

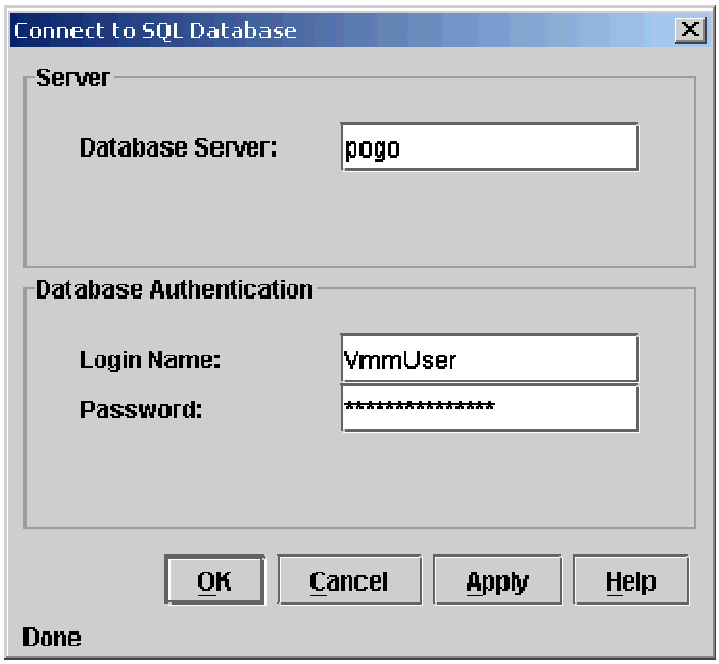
Connect to Database

When VoIP Monitoring Manager is first installed, you need to connect it to the database. You also need to perform this task if you decide to change to a different database (for example, you upgrade to an SQL Server database from the standard MSDE database). This is explained in Migrate Data.

> This setting is for both reading of monitor data and writing of RTCP data.

To connect to a database:

1. From the VoIP Monitoring Manager server interface, select **File > Connect to Database**.



2. Enter the Database Server name, Logon Name, and Password.

   The database server name can be either a name or an IP address. In either case, it must be accessible on your network.

3. Click **OK**.

Manage your licenses

You must log into the WebLM server that manages your Avaya licenses. The license server is required to activate VoIP Monitoring Manager beyond the 90-trial period. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.

Customized Setup

You only need to use these procedures if you are changing the default installation (for example, creating your own database).

Change Monitoring Manager Server

To change the VoIP Monitoring Manager Server that the VoIP Monitoring Manager Client is communicating with:

1. Select **File > Connect to New Server.** The Host Name of Server dialog box appears.
2. Enter the name of the new VoIP Monitoring Manager Server, and click **OK**.

If you are using the VoIP Monitoring Manager Client from a browser, you will be unable to change the server from which the Client is receiving information. The monitor that is displaying the Client must be directly connected to the Server that is running the VoIP Monitoring Manager Server.

Configure Database Tables

You do not need to configure the database tables as part of a normal installation—this happens automatically. You only need to configure the database tables if you initially use the default MSDE database, but then decide to migrate to an SQL Server database.

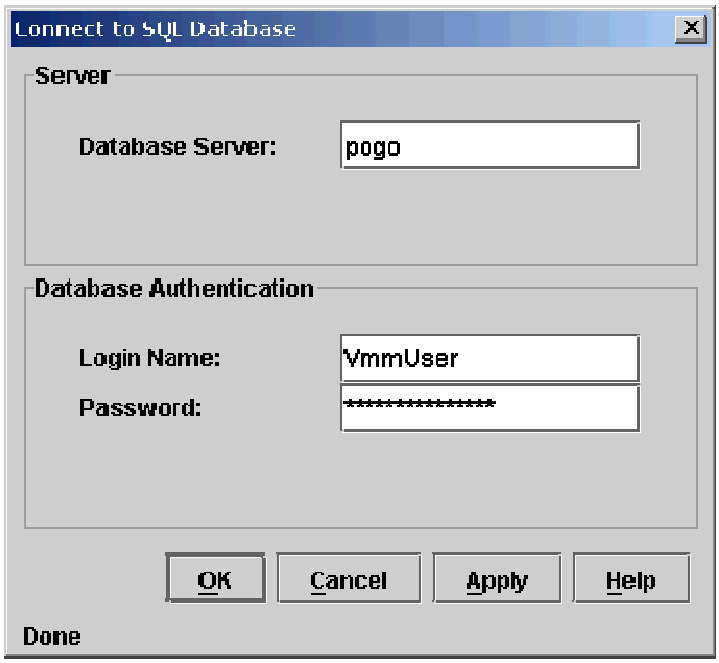
Migrate Data

Use this procedure if you want to migrate VoIP Monitoring Manager data from the standard MSDE database to an SQL Server 2000 database or an SQL Server 2005 database. Reasons for performing this migration include:

- Database content needs to exceed 2 GB.
- You want access to improved management and reporting tools available in SQL Server.
- You want the remote administration capabilities of SQL Server.
- You regularly need a connection pool of more than five connections.

To migrate data:

1. Install SQL Server. VoIP Monitoring Manager supports SQL Server 2000 and SQL Server 2005.
2. Set up the VMM database:
    1. Copy *SetupNewVmmDatabase.zip* to the MS SQL Server machine. (This zip can be found in the VMM installation\SQL folder.)
    2. Extract the zip file and follow the instructions in the extracted *readme.txt* file.
3. Create a backup of the existing MSDE database.
4. Using the standard SQL Server tools, restore the backed-up database as a new SQL Server database. (Alternatively, use the script provided: <*VMM installation directory*>*sql**RestoreVmmDatabase.bat*.)
5. Start Avaya VoIP Monitoring Manager Server.
6. Select **File > Connect to Database**.



7. Enter the Database Server name, Logon Name, and Password. (Note the default VMM login/password created by the setup scripts is **VmmUser/VmmUserPassword**.)
8. Click **OK**.

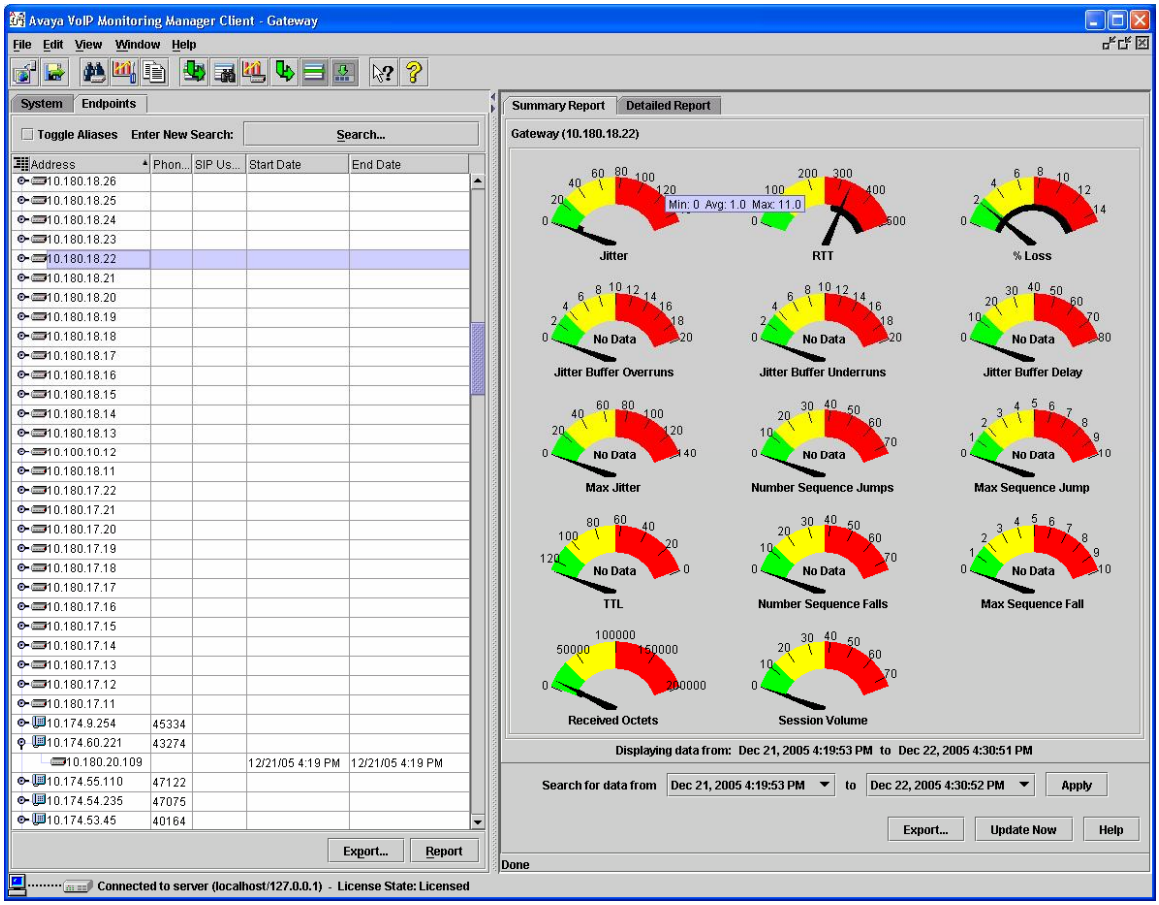
The Avaya VoIP Monitoring Manager Server shows the progress of the connection. When both Server Status and SNMP Agent Status bars at 100%, the connection has been successful.

For security reasons, you must change the VmmUser password. Run the batch file *ChangeVmmUserPassword.bat*, which is included in the zip, to change the password associated with the VmmUser SQL login. Then, reconfigure the VMM Server with the new password.

Overview of VoIP Monitoring Manager Client

VoIP Monitoring Manager Client

The following image displays an example of the VoIP Monitoring Manager Client in use. A search has been completed and a Summary Report is displaying ready for analysis. To familiarize yourself with the environment such as its tools and menus, click on it in the image below.



System Pane

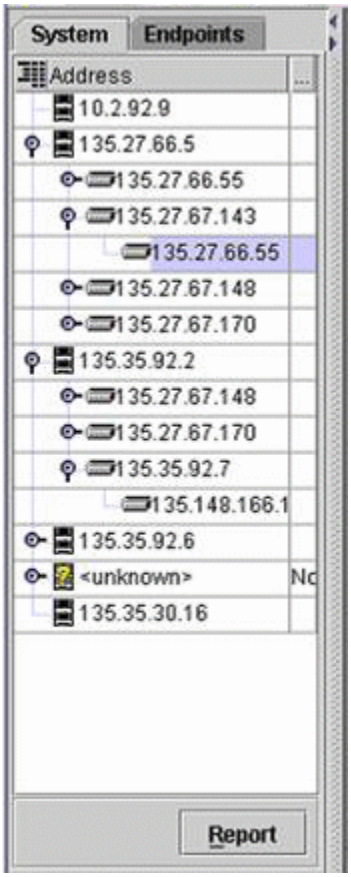
The System pane is populated based on the media gateways that have reported to the VMM server in the last hour (or specified time period).

> Data for the System pane is only obtained over the last hour because this uses an expensive query if the database is large. If your system has a small database, you may want to increase this "look back" time. To increase the "look back" time, you must change the value of the **SystemViewSearchInterval** attribute in the ***VoIPMonMgrClient.ini*** file. The ***VoIPMonMgrClient.ini*** file is located in the VMM installation directory. Note that the value of the **SystemViewSearchInterval** attribute is in hours.

For each object, the System pane displays the following information (if available):

- Name (if you configured friendly names for gateways)
- IP address

The following image shows a sample System pane.



The System pane may contain the following icons:

Gatekeeper

Unknown Gatekeeper

Gateway

From the System pane, you can select a gateway and click the **Report** button to view an aggregated report of all the VoIP sessions over the selected link.

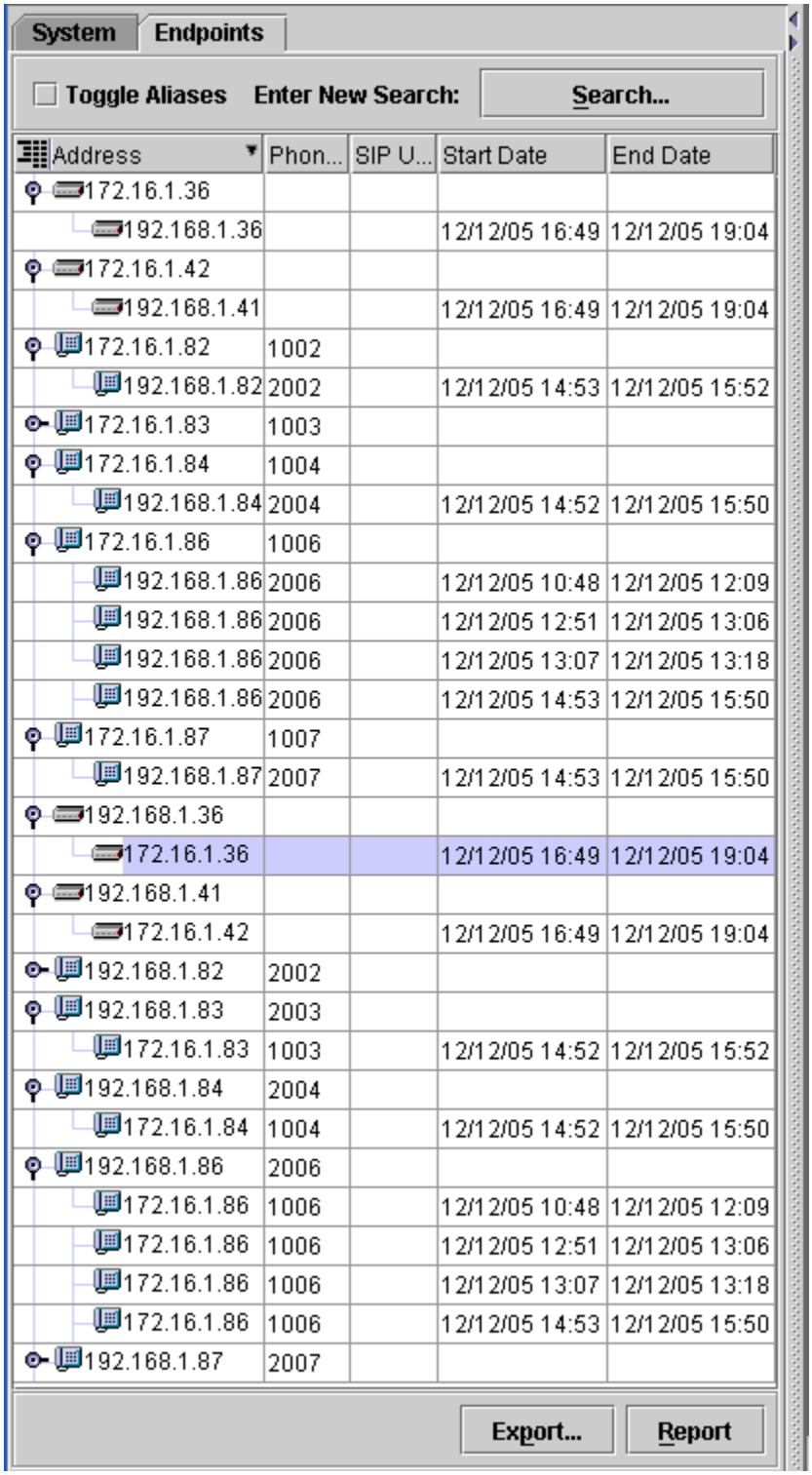
Endpoints Pane

The Endpoints pane displays:

- the list of active endpoints
- the list of endpoints that are the result of a **Search** you performed

From the Endpoints pane, you can click the **Toggle Aliases** check box to view/hide the friendly names for gateways.

The following image shows a sample Endpoints pane.



The Endpoints pane may contain the following icons:

Gateway

IP Phone

Avaya IP Softphone

SIP Phone

Identification information is unavailable for this endpoint

Connection Status

When you start the VoIP Monitoring Manager Client, it attempts to connect to the VoIP Monitoring Manager Server. The results of this connection are displayed in the Status Bar. Some of the possible connection icons are as follows:

	The VoIP Monitoring Manager Client is connected to the VoIP Monitoring Manager Server.
	The VoIP Monitoring Manager Client is not connected to the VoIP Monitoring Manager Server.

Display in Status Bar

When you connect to a new VoIP Monitoring Manager Server, a message displays in the status bar as shown below.

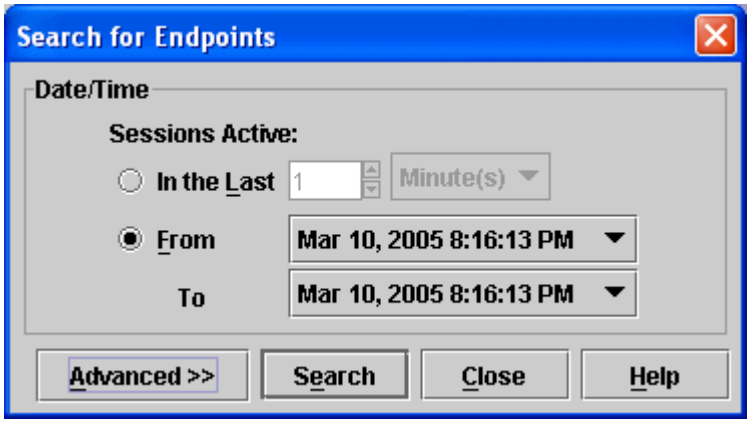
Status Bar

The Status bar is the area of space at the bottom of the VoIP Monitoring Manager Client window that shows the Connection Status and the current license state. You toggle the display of the Status bar either by clicking on its icon on the Tool bar or selecting/deselecting the checkbox in the **View** menu.

Search Dialog Box

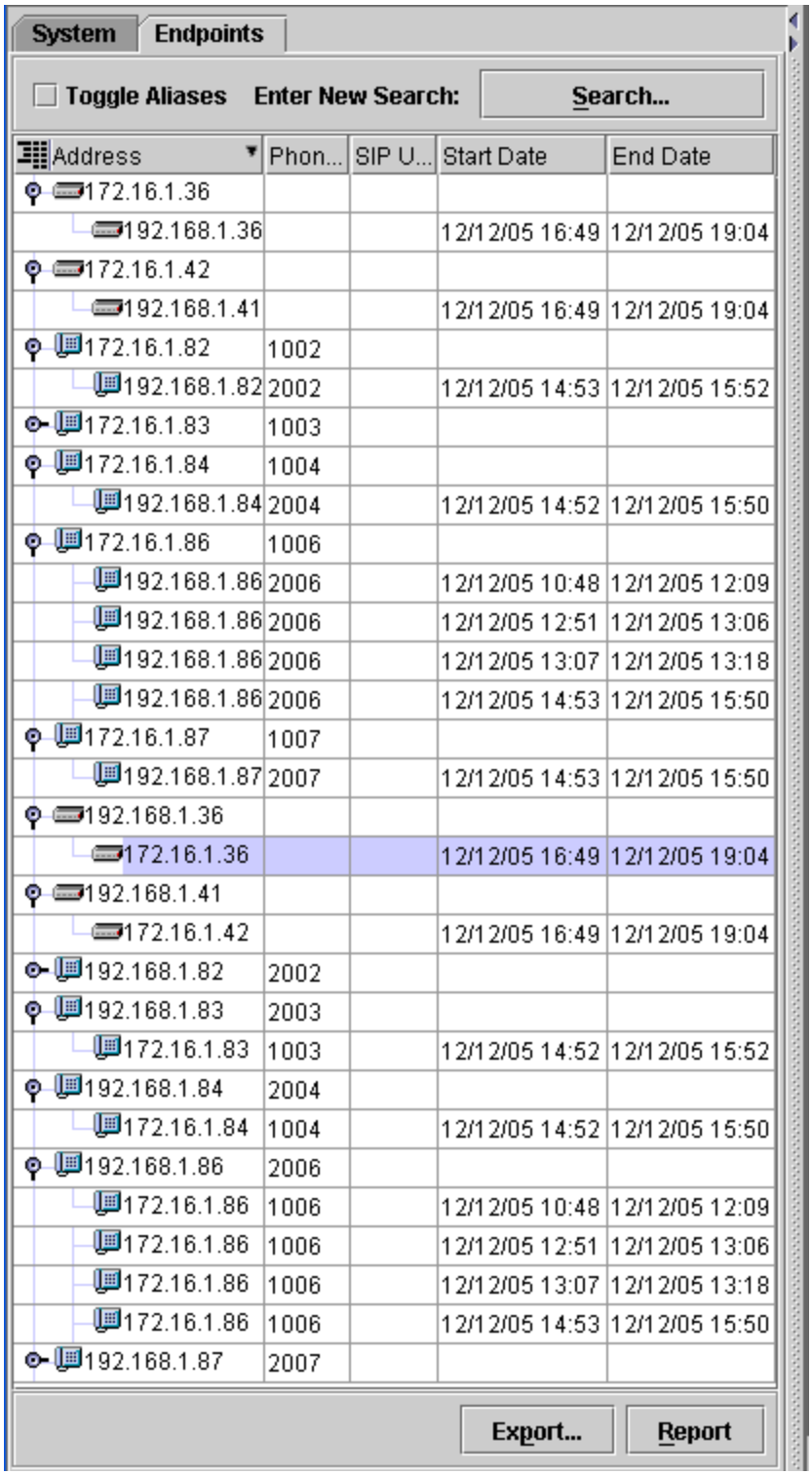
The Search dialog box is where you set your search criteria for gathering endpoints. You access this dialog box by clicking the Search button on the Endpoints tab or selecting **Edit > Search**. A search is based on the time period for the active endpoints. This search could contain endpoints that were active in the last minute, hour, day or month or were active between a date range.

You can use the **Advanced Search** to run a search for a specific phone number, SIP username, network address, or based on a QoS value. Once you have entered the details, click the **Search** button. A Search updates the Results List with the endpoints. You can then select an endpoint and view the report.



Results List

The Results List shown in this image displays a list of endpoints that are a result of the **Search**. You can toggle the display of the Results List by unchecking the option from **View > Results**. You can also reduce and expand the Result Lists pane by pointing your mouse at the right side edge and dragging the edge to the desired size.


System
Endpoints
Toggle Aliases
Enter New Search:
Search...
Address
Phon...
SIP U...
Start Date
End Date
172.16.1.36
192.168.1.36 12/12/05 16:49 12/12/05 19:04
172.16.1.42
192.168.1.41 12/12/05 16:49 12/12/05 19:04
172.16.1.82 1002
192.168.1.82 2002 12/12/05 14:53 12/12/05 15:52
172.16.1.83 1003
172.16.1.84 1004
192.168.1.84 2004 12/12/05 14:52 12/12/05 15:50
172.16.1.86 1006
192.168.1.86 2006 12/12/05 10:48 12/12/05 12:09
192.168.1.86 2006 12/12/05 12:51 12/12/05 13:06
192.168.1.86 2006 12/12/05 13:07 12/12/05 13:18
192.168.1.86 2006 12/12/05 14:53 12/12/05 15:50
172.16.1.87 1007
192.168.1.87 2007 12/12/05 14:53 12/12/05 15:50
192.168.1.36
172.16.1.36 12/12/05 16:49 12/12/05 19:04
192.168.1.41
172.16.1.42 12/12/05 16:49 12/12/05 19:04
192.168.1.82 2002
192.168.1.83 2003
172.16.1.83 1003 12/12/05 14:52 12/12/05 15:52
192.168.1.84 2004
172.16.1.84 1004 12/12/05 14:52 12/12/05 15:50
192.168.1.86 2006
172.16.1.86 1006 12/12/05 10:48 12/12/05 12:09
172.16.1.86 1006 12/12/05 12:51 12/12/05 13:06
172.16.1.86 1006 12/12/05 13:07 12/12/05 13:18
172.16.1.86 1006 12/12/05 14:53 12/12/05 15:50
192.168.1.87 2007
Export...
Report

The Results List pane may contain the following icons:

Gateway

IP phone

Avaya IP Softphone

Avaya SIP phone

View Tool Bar

You can toggle the display of the **Tool Bar** in the VoIP Monitoring Manager Client. Hiding the Tool Bar provides you with more screen space. Toggle this option by selecting/deselecting the **Tool Bar** option from the **View Menu**.

Search Button

To access the **Search** dialog box, perform one of the following steps:

- Click on the **Search button** on the Results List.
- Click the **Search** icon on the **Tool Bar**.
- Select **Edit > Search**.

This opens the Search dialog box, which allows you to run a search for endpoints based on a time period. You can also use the Advanced Search options to narrow your search to match phone number, SIP username, network address, and/ or QoS level.

Getting Started Guide (Client)

Starting VoIP Monitoring Manager Client

You need to ensure that the VoIP Monitoring Manager (VMM) Server is installed and running on the network before you start the VMM Client. If you only have the VMM Server installed, you can also start the VMM Client as a Web Client.

To start VoIP Monitoring Manager Client:

From the PC where the VoIP Monitoring Manager Client software is installed, select **Start > Programs > Avaya > VoIP Monitoring Manager > Client**.

The Avaya VoIP Monitoring Manager Client window appears. Now you can search for endpoints and then view the QoS data in a report format.

How to Use VoIP Monitoring Manager Client

To use the VoIP Monitoring Manager, you must start the VoIP Monitoring Manager Server before you start the Client. Then you can begin to search for endpoints, view reports and begin your analysis.

Using VoIP Monitoring Manager Client, you can:

- Run a Search
- View a Report
- Interpret the Values Using Summary Reports
- Interpret the Values Using Detailed Reports

If you want to become familiar with the application's tools and menus, see VoIP Monitoring Manager Client.

Starting VoIP Monitoring Manager Web Client

The Avaya VoIP Monitoring Manager Client can run as a Web application in a browser. This is useful if you only have the server installed. To run the Avaya VoIP Monitoring Manager Client as a Web application, the following requirements must be met:

- The PC on which the Avaya VoIP Monitoring Manager Server software is installed must be running a Web server. The Apache Web server is automatically installed on the server when the Avaya VoIP Monitoring Manager Server software is installed.
- The Web server must be configured to publish the file to the following VoIP Monitoring Manager installation path:
  C:\Program Files\Avaya\VoIP Monitoring Manager\jars\ClientApplet.htm
- The PC you will use to access the Avaya VoIP Montoring Manager Server must be able to connect to the VMM server via a Web browser and have the following software installed:
  - Microsoft Internet Explorer 6 or later
  - SUN Java 2 Runtime Environment, SE v1.4.2_06

For more information see the topic About the VoIP Monitoring Manager Web Client

To Start Web Client

From your browser, type in the following url:

```
Http://VMMServerMachineName/VoIPMonMgr/ClientApplet.html
```

where VMMServerMachineName = the machine running the VMM Server. This url points to the machine running the VMM Server.

If you do not have the Sun Java Plug-in installed, you are prompted to install it.

To exit the Web Client, just close the browser.

There are limitations in using the VMM Web Client. These are imposed by the security restrictions associated with running unsigned applets. The limitations are:

- You can only access one monitor that is directly connected to the server running the VMM Server.
- You cannot:
  - Connect to a new server.
  - Use the Copy functionality.
  - Persist the settings from the Report Properties dialog box.
  - Log to the Windows event log or files.
  - Configure aliases for gateways on the client system.

Run a Search

The first action required when using the VoIP Monitoring Manager Client is to search for endpoints. You can search endpoints active from a point in time in the past or between a date range. You can also use the Advanced Search options to narrow the search based on phone number, SIP username, network addresses, or QoS value. Once you have completed your search, the Results List display the list of endpoints that match your search criteria. You can then view a report for an endpoint in the Results List.

To Run a Search

1. Perform one of the following steps:
   - Select **Edit > Search**.
   - Click **Search** on the Endpoints pane.

   The Search dialog box appears.
2. From the **Search** dialog box, click the drop-down arrow to select the time period for active endpoints. The default is 1 minute, but you can select hours, days, weeks, or months.
3. If you want to select a date range of active endpoints, click **From** and click the calendar(s) drop-down arrow to open the calendar.

4. From the calendars, select the **start** (from) and **end date** (to) of the range. You can select hours, minutes, seconds, and AM/PM. You can also use the arrow buttons to scroll through the months and years.

5. Click **Search**. The Results List updates with a list of endpoints that match your search criteria. Now, you can select an endpoint and view its report.

View a Report

You can generate reports for endpoints and media gateways.

Endpoint Reports

After you run a search, you can view the report on selected endpoints and endpoints involved in a session. There are two types of Endpoint reports: Summary Reports and Detailed Reports.

To View the QoS Data for an Endpoint

1. From the **Results List,** select an **endpoint** or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.

2. Click **Report**. The Report dialog box opens.

Media Gateway Link Reports

From the System pane, you can select a media gateway and click the **Report** button to view an aggregated report of all the VoIP sessions over the selected link. There are three types of Media Gateway Link reports: Summary Media Gateway Link Report, Detailed Media Gateway Link Report, and Trace Routes Media Gateway Link Report.

How to... (Client)

Connect to New Server

The Connect to New Server option enables you to change the VMM server to which the VoIP Monitoring Manager Client connects, so that you can analyze endpoints that are reporting to a different server. This option is not available when using the VoIP Monitoring Manager Web Client.

To Change the VoIP Monitoring Manager Server

1. Select **File > Connect to a New Server**. The Host Name Server dialog box opens.
2. From the Host Name Server dialog box, type in the name of the VoIP Monitoring Manager Server.
3. Click **OK** to save the changes. The Connection in Progress dialog box displays. The VoIP Monitoring Manager Client starts connecting to the VoIP Monitoring Manager Server you specified.

When the connection is made to the VMM server, the Connection Status will display the network as being **Ready**. If the connection to the VoIP Monitoring Manager Server is unsuccessful, you will be prompted to check if the VoIP Monitoring Manager Server is available and to try again.

Run a Search

The first action required when using the VoIP Monitoring Manager Client is to search for endpoints. You can search endpoints active from a point in time in the past or between a date range. You can also use the Advanced Search options to narrow the search based on phone number, SIP username, network addresses, or QoS value. Once you have completed your search, the Results List display the list of endpoints that match your search criteria. You can then view a report for an endpoint in the Results List.

To Run a Search

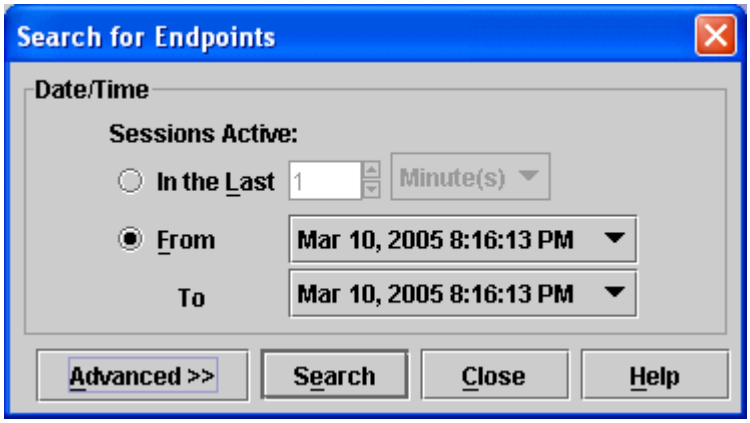
1. Perform one of the following steps:
   - Select **Edit > Search**.
   - Click **Search** on the Endpoints pane.

   The Search dialog box appears.
2. From the **Search** dialog box, click the drop-down arrow to select the time period for active endpoints. The default is 1 minute, but you can select hours, days, weeks, or months.
3. If you want to select a date range of active endpoints, click **From** and click the calendar(s) drop-down arrow to open the calendar.
4. From the calendars, select the **start** (from) and **end date** (to) of the range. You can select hours, minutes, seconds, and AM/PM. You can also use the arrow buttons to scroll through the months and years.
5. Click **Search**. The Results List updates with a list of endpoints that match your search criteria. Now, you can select an endpoint and view its report.

Search Dialog Box

The Search dialog box is where you set your search criteria for gathering endpoints. You access this dialog box by clicking the Search button on the Endpoints tab or selecting **Edit > Search**. A search is based on the time period for the active endpoints. This search could contain endpoints that were active in the last minute, hour, day or month or were active between a date range.

You can use the **Advanced Search** to run a search for a specific phone number, SIP username, network address, or based on a QoS value. Once you have entered the details, click the **Search** button. A Search updates the Results List with the endpoints. You can then select an endpoint and view the report.

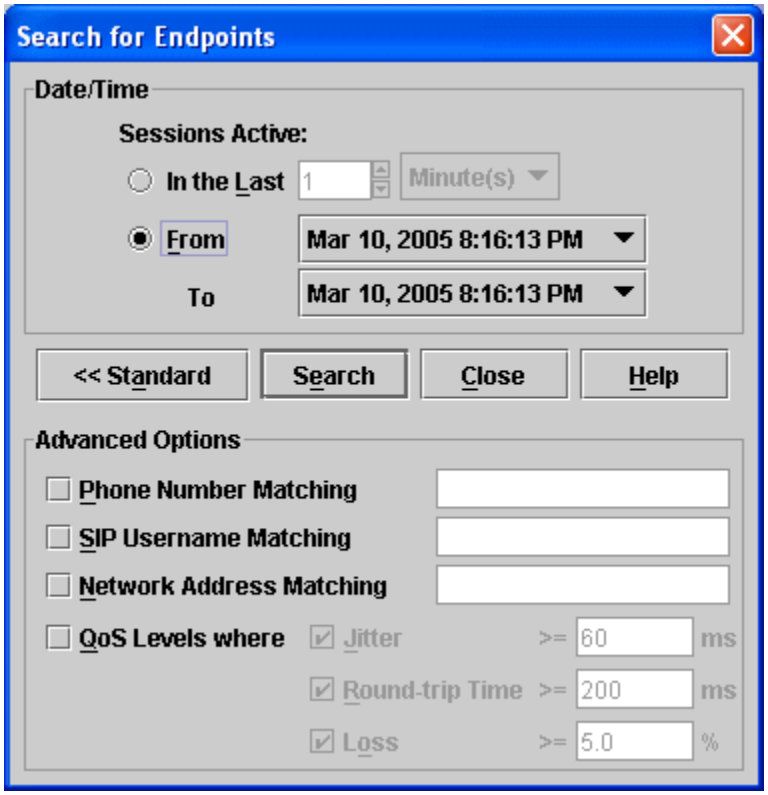


Advanced Search

The Advanced Search enables you to search for endpoints matching a phone number, SIP username, network address, or QoS value. You can select one or more of the search options, and you can enter more than one phone number or network address.

To Run an Advanced Search

1. From the **Search** dialog box, click **Advanced Search**. If the Search dialog box is not visible on the screen, click **Search** to display the Search dialog box.
2. Check one or more of the checkboxes and/or type a value in the fields. If more than one item is selected, the results returned will match all the parameters set (for example, Jitter >= 300 and RTT >= 350 for a specified phone number).
3. Click the **Search** button. The Results List updates.



Search for a Specific Network Address

You can specify in your search to display endpoints that match an IP Address or hostname by entering the address or hostname in the Advanced Search options. This is useful for narrowing your search to a limited number of results displaying in the Results List.

You can enter:

- A range of IP addresses such as 123.4.122.122 – 123.4.122.225.
- A list of addresses that are separated by commas such as 123.4.102.120, 223.4.122.122, belibot.mycomputer.com.
- A part of the IP address, you can use an asterisk (*) as a substitution. For example; if you enter 123.*.*.225, it will find all addresses that start with 123 and end with 225 such as 123.4.122.225 and 123.4.190.225.
- A part of the name such as *belibot* for *belibot.mycomputer.com*. However, in this situation the search will only find hostnames in the same domain.

Search for a Specific Phone Number

You can specify in your search to display endpoints that match a specific phone number by entering in the phone number in the Advanced Search options. This is useful for narrowing your search to a limited number of results displaying in the Results List.

You can:

- Enter commas to separate numbers e.g. **9835, 9872**. If you include spaces between numbers, VoIP Monitoring Manager will remove them. So, if you enter **9835, 9822 9872**, VoIP Monitoring Manager will remove the space between **9822** and **9872** and then search for **9835** and **98229872**.
- Use dashes to specify a range of phone numbers e.g. **2000 – 8000**.
- Enter a question mark (?) or asterisk (*) as a wild card. It is useful for substituting numbers in your search. The question mark can be used multiple times. However, each ? substitutes for exactly one character. An asterisk (*) substitutes for 0 or more characters. Wild cards cannot be used in ranges.

Example Wild Card Searches

- ?345 = Finds all extensions that are four digits long and end with 345. (? substitutes for exactly one character.)
- 9??? = Finds all the extensions from 9000 – 9999.
- 9* = Finds all the extensions that start with 9.

Search for a Specific SIP Username

You can specify in your search to display endpoints that match a specific SIP username by entering the SIP username in the Advanced Search options. This is useful for narrowing your search to a limited number of results displaying in the Results List.

You can:

- Enter a question mark (?) or asterisk (*) as a wild card. It is useful for substituting characters in your search. The question mark can be used multiple times. However, each ? substitutes for exactly one character. An asterisk (*) substitutes for 0 or more characters. Wild cards cannot be used in ranges.

Example Wild Card Search

- B??? = Finds all the SIP usernames that consist of four characters and begin with the letter B.
- B* = Finds all the SIP usernames that start with the letter B.

Search Using Quality of Service (QoS) Values

You can specify in your search to display endpoints that have QoS values greater than or equal to a given threshold by using the Advanced Search options. The Results List will only display those endpoints that contain the QoS data you have specified. This is useful for narrowing your search to a limited number of results that you will need to analyze.

The default ranges are as follows:

•□□□Jitter	Greater than or equal to 60 ms
•□□□Round Trip Time	Greater than or equal to 200 ms
•□□□Packet Loss	Greater than or equal to 5%

View Results List

The Results List displays the results of your search. You can toggle the display of the Results List. Hiding the Results List creates more space so that it is easier to see the reports. You toggle the display of the Results List either by clicking on this icon on the **Tool Bar** or selecting/deselecting the checkbox in the **View** menu.

Export Result List

You can export the data in the results list to a comma separated value (csv) file.

The exported data contains records for every endpoint and every session that is displayed in VoIP Monitoring Manager. Opening or closing session folders (to show or hide the endpoints) does not affect the data that is exported.

You can open this file in most database and spreadsheet programs such as Microsoft Excel. Exporting the data to a spreadsheet enables you to manipulate the data so you can create your own reports. Click this link to see an example (Adobe Acrobat 5 or later required – the page has been split into three because of its width). You can use the sorting, counting, and calculation features of Microsoft Excel to create your own reports from this raw data.

The data exported is divided into 3 tables:

- Session Table
- Time-varying Data Table
- Trace Route Table

To Export Data from the Result List

1. Perform one of the following steps:
    - From the File menu, select **Export Result List**.
    - Click the **Export** button located at the bottom of the **Result List**.

    Tip: If you want to limit the data that is exported, narrow down your search so that less data displays in the Result List.
2. In the Save as dialog box, navigate to a folder.
3. In the **File name** box, type a name for the file.

4. Click **Save as**. The file saves with the CSV extension.
5. From Microsoft Excel, open the file. From here you can build your own report.

> Microsoft Excel can only handle 65,536 rows of data. If your exported data file contains more rows, you will need to write a script that splits the data into smaller files before you import the data into Excel.

Creating Reports with Exported Data

You can export the data from the Result List and/or Report dialog boxes to Microsoft Excel. Using Microsoft Excel you can create your own reports as shown in the linked example. This report was created by using Microsoft Excel's calculation features. It includes averaging results, counting the number of sessions and unique participants, setting filters to determine the longest sessions, and creating a line graph to visually demonstrate the information. You can create your own reports from the exported data. click this link to see an example (Adobe Acrobat reader is required).

View Active Endpoints

You can view all active endpoints by clicking on this icon on the **Tool Bar** or selecting this option from the **View Menu**. The **Results List** is updated with all currently active endpoints.

View Status Bar

The Status Bar is the area of space at the bottom of the VoIP Monitoring Manager Client that shows the Connection Status and the current license state. You toggle the display of the Status bar either by clicking on its icon on the Tool bar or selecting/deselecting the checkbox in the **View** menu.

Update System View

To update information displayed on the System pane, click the **Update System View** icon. This icon is located on the Tool Bar and the menu option can be accessed from **View > Refresh System View**.

Configure Friendly Names for Gateways

By default, VMM provides an IP address (when available) for each gateway. To make it easier to identify gateways, you can assign an alias (a "friendly" name) for each gateway. When assigned, the alias for a gateway will be displayed in the Label column on the System pane. However, on the Endpoints pane, you can use the **Toggle Aliases** check box to view or hide the aliases.

You can assign aliases on

- **a per-server basis**
  If you configure aliases on a per-server basis, the aliases will be displayed on all VMM clients that access that VMM server.
- **a per-client basis**
  If you configure aliases on a per-client basis, each VMM client will use its own aliases for the gateways. Even though each VMM client will view the same gateways, each VMM client will have its own alias for each gateway.
- **both a per-server basis and a per-client basis**
  If you configure aliases on both a per-server basis and a per-client basis, the VMM client will use the alias from the VMM server if that VMM client does not have an alias specified for the gateway. If both the VMM server and the VMM client have specified an alias for

the same gateway, VMM client will use its alias. In this configuration, the alias specified in the VMM client will always take precedence over the alias specified in the VMM server.

You can configure aliases for gateways in one of the following ways:

- from the VMM Server interface
- from the VMM client
- via a configuration file

Configuring Aliases from the VMM Server Interface

From the VMM Server interface, you can:

- add aliases
- change aliases
- delete aliases

To configure aliases for gateways, perform the following steps:

1. From the Edit menu, select **Configure Aliases**. The Alias Configuration dialog box appears.
2. Make your changes for each gateway.
3. When finished, click **OK**.

Configuring Aliases from the VMM Client

From the VMM client, you can:

- add aliases
- change aliases
- delete aliases

To configure aliases for gateways, perform the following steps:

1. From the Edit menu, select **Configure Aliases**. The Alias Configuration dialog box appears.
2. Make your changes for each gateway.
3. When finished, click **OK**.

Configuring Aliases via a Configuration File

To configure aliases for gateways, you must create a gateway alias configuration file and assign an alias to the IP address of each gateway you want. In the configuration file, you define an alias for a gateway by entering the IP address of the gateway, followed by the alias you want to use. Be sure to enter one IP address and alias per line in this file.

For example, suppose you have gateways at IP addresses 192.168.33.50, 192.168.37.89, and 192.168.56.22, and you want to assign an alias to each gateway. In the gateway alias configuration file, you would enter the following information:

```
192.168.33.50 Bob
192.168.37.89 Alice
192.168.56.22 Jane
```

Once you create and save the gateway alias configuration file, you must specify the name of this file as the value of the **FriendlyPath** attribute in the server and/or client initialization files. By default, in both the VMM server initialization file and the VMM client initialization file, the

FriendlyPath attribute is set to **FriendlyLabelsServer.ini** (FriendlyPath=FriendlyLabelsServer.ini).

VMM server uses the initialization file ***VoIPMonMgrServer.ini***. VMM client uses the initialization file ***VoIPMonMgrClient.ini***. These initialization files are located in the VMM installation directory.

NOTE:
The gateway alias configuration file must be located in the same folder as the VMM initialization file (that is, VoIPMonMgrServer.ini or VoIPMonMgrClient.ini).

About Dialog

This dialog box shows

- the version of VMM
- the current license state (that is, whether you are using a valid license or you are running VMM in evaluation mode)
- the number of licenses purchased
- the number of phones at the local server. This number represents the phones that reported to VMM in the last 28 days. This number will increase if you move phones (for example, change extensions or IP addresses). In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, this will not be a problem.
- the number of phones at the local server that exceed the license (that is, the number of phones that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more phones stored in the database than licenses purchased.
- the number of media gateways at the local server. This number represents the media gateways that reported to VMM in the last 28 days.
- the number of media gateways at the local server that exceed the license (that is, the number of media gateways that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more media gateways stored in the database than licenses purchased.

Avaya provides a 90-day trial version of VoIP Monitoring Manager. After 90 days, VoIP Monitoring Manager stops collecting RTCP data. You have the option of purchasing the VoIP Monitoring Manager license key. This key is required to fully activate the VoIP Monitoring Manager beyond the 90-day trial period. When a license key is purchased, an instance of WebLM License Server is required to manage the license key. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.

Working with Reports (Client)

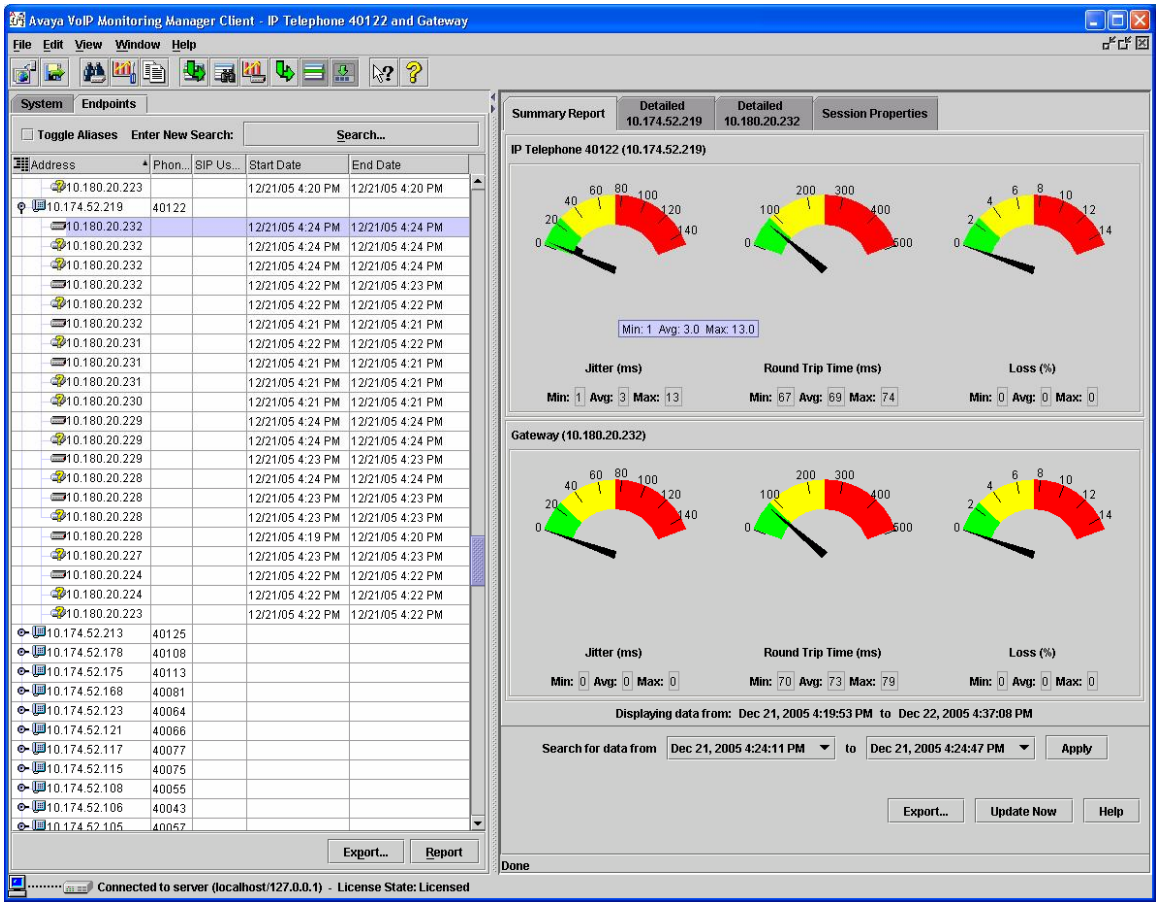
About Summary Reports

The Summary Report displays the QoS data as a reading on a gauge. The green segment of the gauge indicates values that reflect acceptable voice quality measured. The amber segment warns you of degraded voice quality levels and the red segment indicates unacceptable voice quality levels measured. The needle on the gauge shows the average values measured and the black inner arc shows the range of values measured. To edit the default range displayed on the gauges, use the Report Properties dialog.

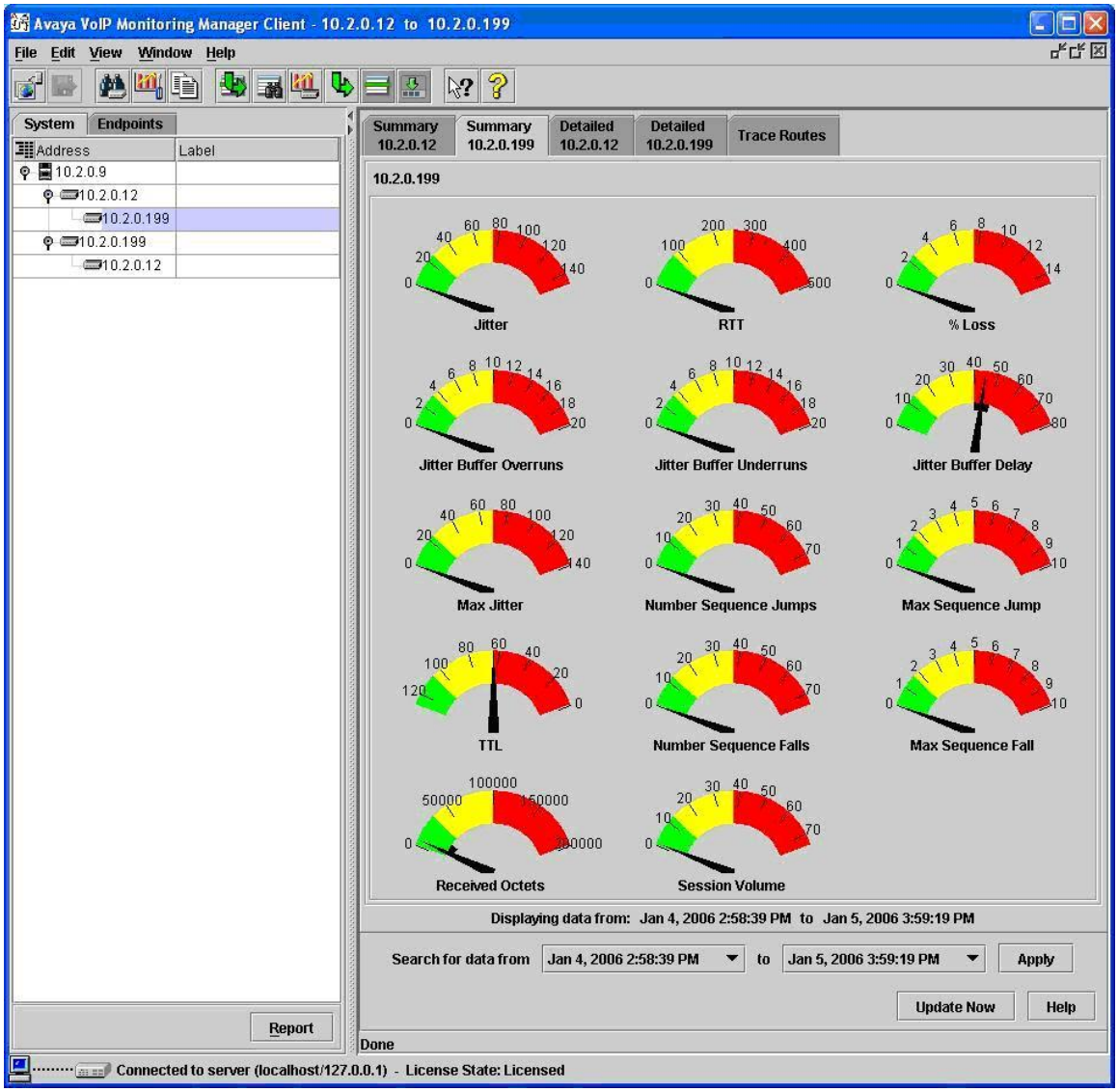
Summary Report Features

- **Displays information** such as the type of endpoint and the phone number.
- **Displays start and end dates** at the bottom of the report. These dates can be altered to narrow or lengthen the date range. This will cause the data to show more or less detail in the report.

The following is an example of a Summary Report for endpoints:


Avaya VoIP Monitoring Manager Client - IP Telephone 40122 and Gateway
File Edit View Window Help
System Endpoints
Toggle Aliases Enter New Search: Search...
Address Phon... SIP Us... Start Date End Date
Summary Report
Detailed 10.174.52.219
Detailed 10.180.20.232
Session Properties
IP Telephone 40122 (10.174.52.219)
Min: 1 Avg: 3.0 Max: 13.0
Jitter (ms)
Min: 1 Avg: 3 Max: 13
Round Trip Time (ms)
Min: 67 Avg: 69 Max: 74
Loss (%)
Min: 0 Avg: 0 Max: 0
Gateway (10.180.20.232)
Jitter (ms)
Min: 0 Avg: 0 Max: 0
Round Trip Time (ms)
Min: 70 Avg: 73 Max: 79
Loss (%)
Min: 0 Avg: 0 Max: 0
Displaying data from: Dec 21, 2005 4:19:53 PM to Dec 22, 2005 4:37:08 PM
Search for data from Dec 21, 2005 4:24:11 PM to Dec 21, 2005 4:24:47 PM Apply
Export... Update Now Help
Export... Report
Done
Connected to server (localhost/127.0.0.1) - License State: Licensed

The following is a sample Summary Report for a Media Gateway Link:



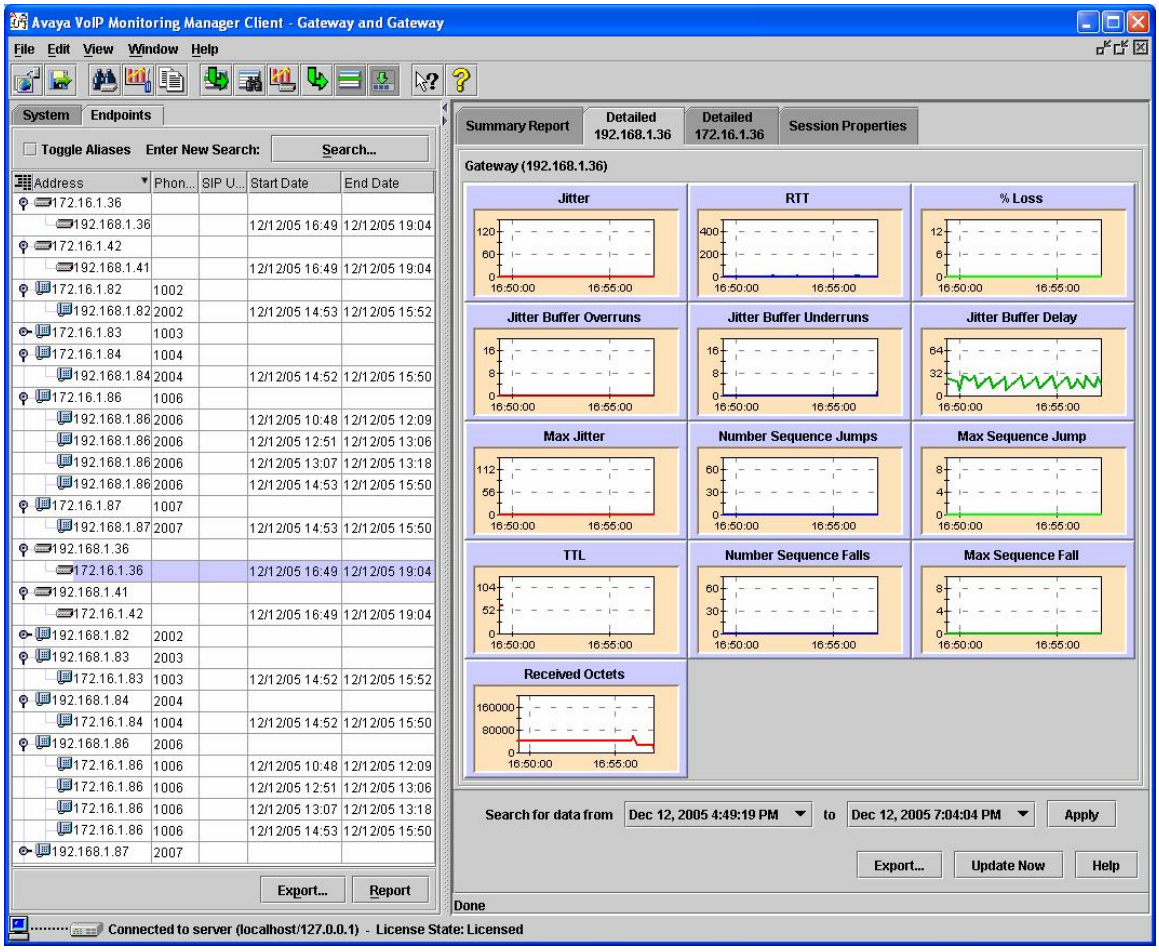
About Detailed Reports

A Detailed Report shows how the QoS values change during the call and when this occurred. This information is displayed on a line graph for each QoS parameter. The X-axis shows the time range, and the Y-axis shows the value for each of the QoS parameters. The upper values on the Y-axis indicate unacceptable limits. Each point on the line graph represents the maximum value since the last point displayed.

Detailed Report Features

- **A tool tip** enables you to point your mouse at the data on the line graph to see the exact data measured.
- Show more or less detail by altering the date range. These dates can be altered to narrow or lengthen the date range. This causes the data to show respectively more or less detail in the report.
- To zoom in on a specific area of a graph, press and hold the SHIFT key and drag the mouse on the graph. To reset the view of a graph, right-click on the graph, and select **Reset View** from the menu. To reset the view of all the graphs, select **Reset View** from the View menu.
- To pan the data points in a graph, press and hold the ALT key and drag the mouse on the graph.

The following is an example of a Detailed Report for an endpoint.

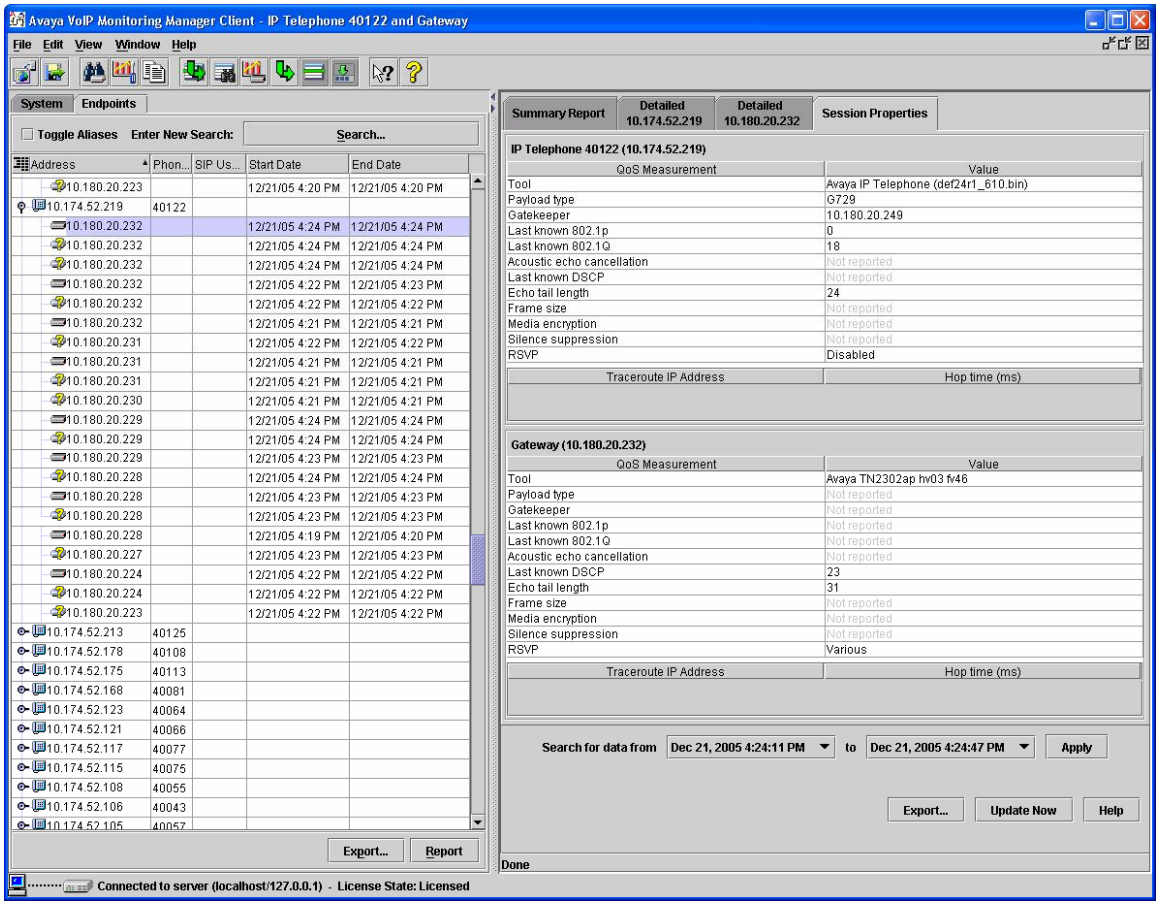


About Session Properties

The Session Properties tab displays the following static properties of the current session:

- tool
- payload type
- gatekeeper
- last known 802.p
- last known 802.1Q
- acoustic echo cancellation
- last known DSCP
- echo tail length
- frame size
- media encryption
- silence suppression
- RSVP

The following is an example of the Session Properties tab.


Avaya VoIP Monitoring Manager Client - IP Telephone 40122 and Gateway
File Edit View Window Help
System Endpoints
Toggle Aliases Enter New Search: Search...
Address Phon... SIP Us... Start Date End Date
Summary Report Detailed 10.174.52.219 Detailed 10.180.20.232 Session Properties
IP Telephone 40122 (10.174.52.219)
QoS Measurement Value
Tool Avaya IP Telephone (def24r1_610.bin)
Payload type G729
Gatekeeper 10.180.20.249
Last known 802.1p 0
Last known 802.1Q 18
Acoustic echo cancellation Not reported
Last known DSCP Not reported
Echo tail length 24
Frame size Not reported
Media encryption Not reported
Silence suppression Not reported
RSVP Disabled
Traceroute IP Address Hop time (ms)
Gateway (10.180.20.232)
QoS Measurement Value
Tool Avaya TN2302ap hv03 fv46
Payload type Not reported
Gatekeeper Not reported
Last known 802.1p Not reported
Last known 802.1Q Not reported
Acoustic echo cancellation Not reported
Last known DSCP 23
Echo tail length 31
Frame size Not reported
Media encryption Not reported
Silence suppression Not reported
RSVP Various
Traceroute IP Address Hop time (ms)
Search for data from Dec 21, 2005 4:24:11 PM to Dec 21, 2005 4:24:47 PM Apply
Export... Update Now Help
Export... Report
Done
Connected to server (localhost/127.0.0.1) - License State: Licensed

To view the Session Properties

1. From the Result List on the Endpoints tab, expand a call and select a **session** from the list.
2. Click **Report**. The Report window displays.
3. In the Report window, click the **Session Properties** tab. The Session Properties displays.

Difference Between Endpoint and Session Reports

The QoS data that displays on an endpoint report is an aggregation of all the sessions that are active at this endpoint.

Single Endpoint Reports Show Multiple Sessions

Some endpoints (such as media gateways) can participate in multiple concurrent sessions, so a high value on a single endpoint report indicates that one or more of the sessions is/was experiencing degradation of quality. It does not indicate which session.

Session Reports Display Endpoints for Only that Session

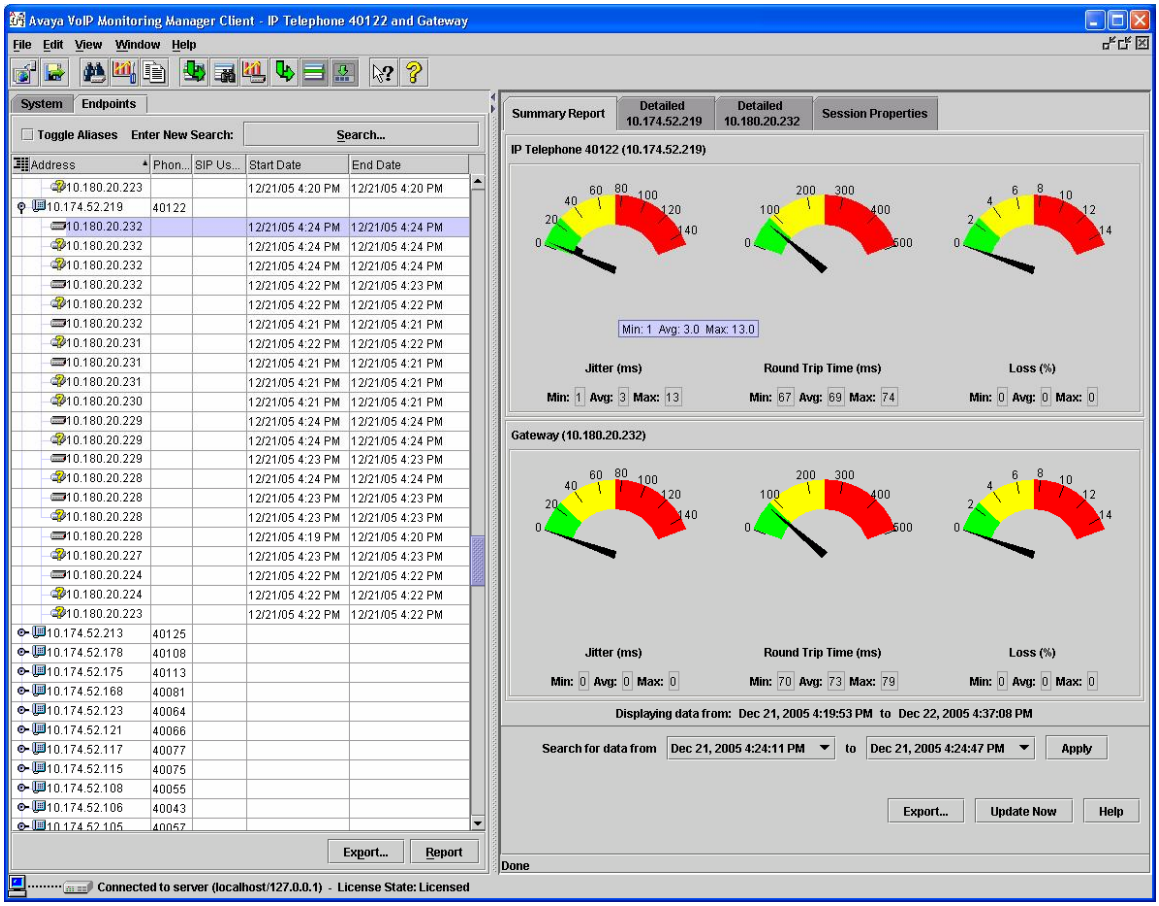
In contrast, a report showing both endpoints involved in the session displays the QoS data as experienced by both endpoints for that session only. To isolate problems, you need to narrow your search by either searching for a specific QoS value or altering the date of the report.

Summary Session Report

Summary Reports show the QoS data as a reading on a gauge. The needle on the gauge shows the average values measured and the black inner arc shows the minimum and maximum values measured.

Summary Reports for Endpoints

In a Summary Report for endpoints, the parent endpoint involved in the session displays in the top report with the child endpoint below. Each of the three QoS parameters is displayed on a separate gauge. The following is an example of a Summary Report for an endpoint:

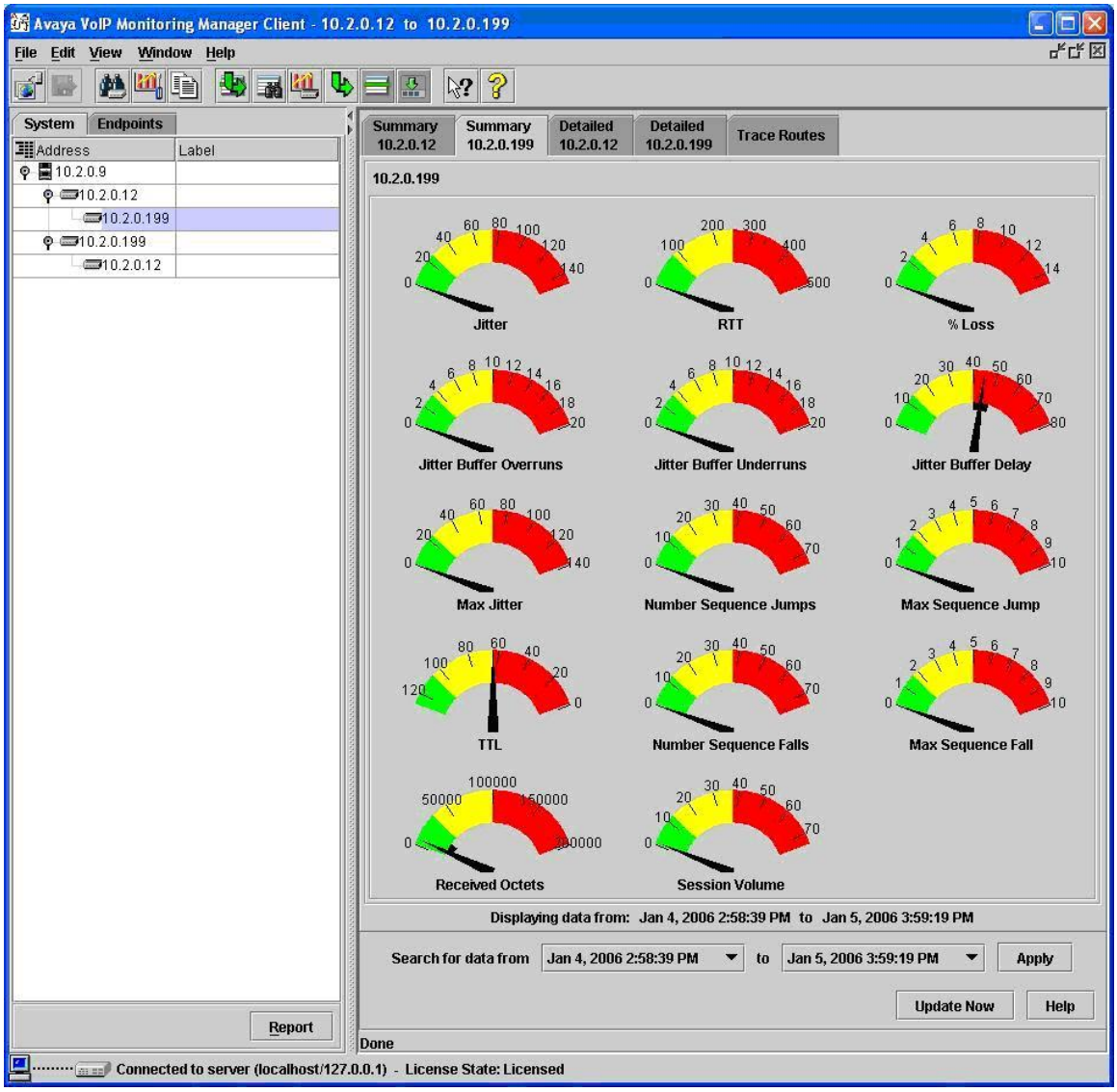

Avaya VoIP Monitoring Manager Client - IP Telephone 40122 and Gateway
File Edit View Window Help
System Endpoints
Toggle Aliases Enter New Search: Search...
Address Phon... SIP Us... Start Date End Date
10.180.20.223 12/21/05 4:20 PM 12/21/05 4:20 PM
10.174.52.219 40122
10.180.20.232 12/21/05 4:24 PM 12/21/05 4:24 PM
10.180.20.232 12/21/05 4:24 PM 12/21/05 4:24 PM
10.180.20.232 12/21/05 4:24 PM 12/21/05 4:24 PM
10.180.20.232 12/21/05 4:22 PM 12/21/05 4:23 PM
10.180.20.232 12/21/05 4:22 PM 12/21/05 4:22 PM
10.180.20.232 12/21/05 4:21 PM 12/21/05 4:21 PM
10.180.20.231 12/21/05 4:22 PM 12/21/05 4:22 PM
10.180.20.231 12/21/05 4:21 PM 12/21/05 4:21 PM
10.180.20.231 12/21/05 4:21 PM 12/21/05 4:21 PM
10.180.20.230 12/21/05 4:21 PM 12/21/05 4:21 PM
10.180.20.229 12/21/05 4:24 PM 12/21/05 4:24 PM
10.180.20.229 12/21/05 4:24 PM 12/21/05 4:24 PM
10.180.20.229 12/21/05 4:23 PM 12/21/05 4:23 PM
10.180.20.228 12/21/05 4:24 PM 12/21/05 4:24 PM
10.180.20.228 12/21/05 4:23 PM 12/21/05 4:23 PM
10.180.20.228 12/21/05 4:23 PM 12/21/05 4:23 PM
10.180.20.228 12/21/05 4:19 PM 12/21/05 4:20 PM
10.180.20.227 12/21/05 4:23 PM 12/21/05 4:23 PM
10.180.20.224 12/21/05 4:22 PM 12/21/05 4:22 PM
10.180.20.224 12/21/05 4:22 PM 12/21/05 4:22 PM
10.180.20.223 12/21/05 4:22 PM 12/21/05 4:22 PM
10.174.52.213 40125
10.174.52.178 40108
10.174.52.175 40113
10.174.52.168 40081
10.174.52.123 40064
10.174.52.121 40066
10.174.52.117 40077
10.174.52.115 40075
10.174.52.108 40055
10.174.52.106 40043
Export... Report
Summary Report
Detailed 10.174.52.219
Detailed 10.180.20.232
Session Properties
IP Telephone 40122 (10.174.52.219)
Min: 1 Avg: 3.0 Max: 13.0
Jitter (ms)
Min: 1 Avg: 3 Max: 13
Round Trip Time (ms)
Min: 67 Avg: 69 Max: 74
Loss (%)
Min: 0 Avg: 0 Max: 0
Gateway (10.180.20.232)
Jitter (ms)
Min: 0 Avg: 0 Max: 0
Round Trip Time (ms)
Min: 70 Avg: 73 Max: 79
Loss (%)
Min: 0 Avg: 0 Max: 0
Displaying data from: Dec 21, 2005 4:19:53 PM to Dec 22, 2005 4:37:08 PM
Search for data from Dec 21, 2005 4:24:11 PM to Dec 21, 2005 4:24:47 PM Apply
Export... Update Now Help
Done
Connected to server (localhost/127.0.0.1) - License State: Licensed

Summary Reports for Media Gateways

For media gateways, the a Summary Report displays the following aggregate information for all of the VoIP sessions for the selected media gateway:

- Jitter
- RTT
- % Loss
- Jitter Buffer Overruns
- Jitter Buffer Underruns
- Jitter Buffer Delay
- Max Jitter
- Number Sequence Jumps
- Max Sequence Jump
- TTL
- Number Sequence Falls
- Max Sequence Fall
- Received Octets
- Session Volume

A Summary Report is available for each media gateway. The following is an example of a Summary Report for a media gateway:



Detailed Reports for Endpoints

Detailed Reports show how the QoS values change during the call and when these changes occurred. This information is displayed on a line graph for each QoS parameter. The X-axis shows the time range, and the Y-axis shows the value of the QoS parameter. Each point on the line graph represents the maximum value since the last point displayed.

Detailed Reports provide a tool tip that enables you to point your mouse at the data on the line graph to see the exact data measured. You can also alter the date range to show more or less detail.

You interpret the Detailed Report by noting where the sampled points for each QoS value appear on the line graph and when this may have occurred. The default upper values on the Y-axis indicate unacceptable limits. Select **Edit>Report Properties** to change the lower and upper limits of each QoS value.

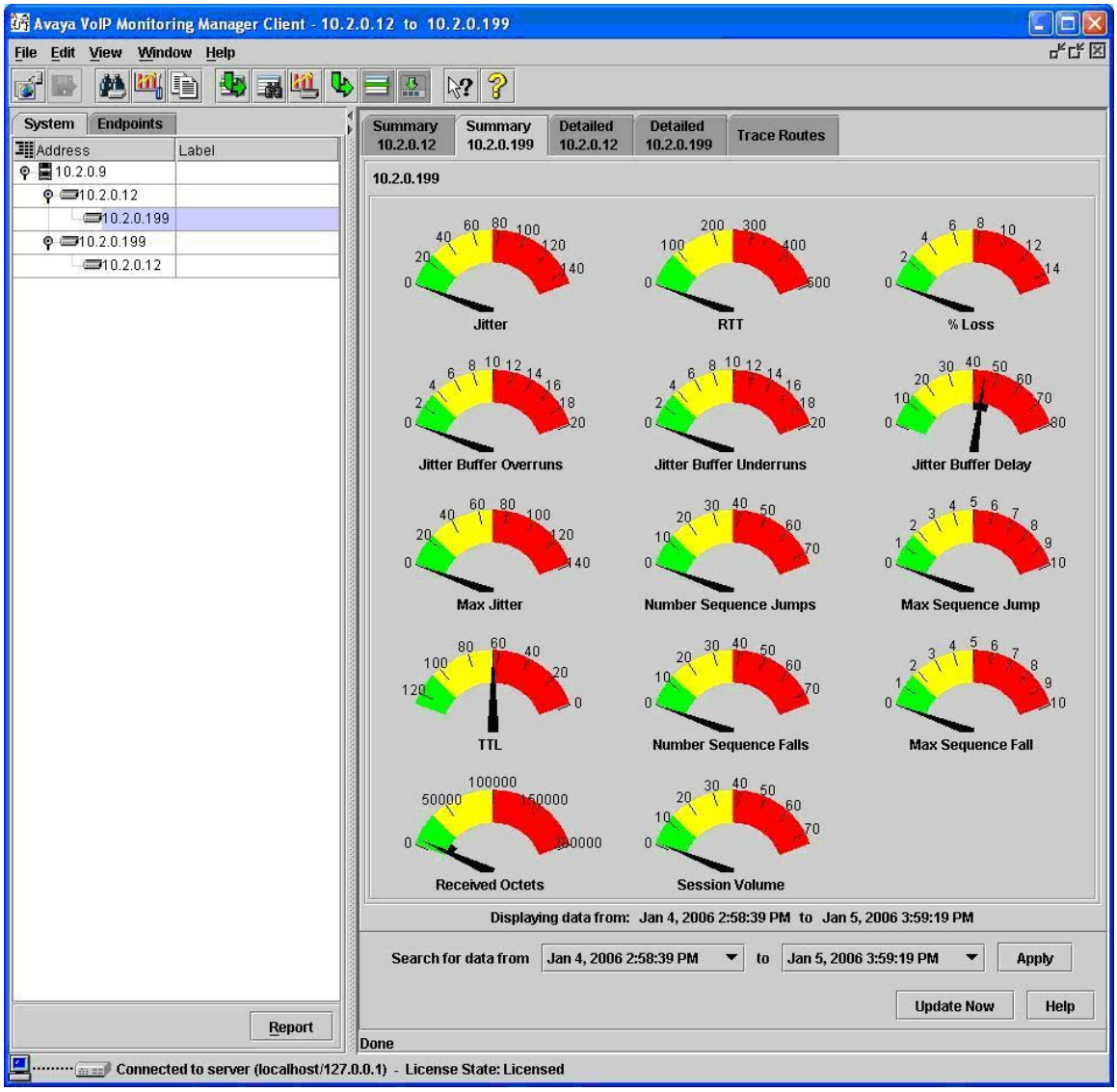
To view a Detailed Report for an endpoint, click the **Detailed Report** tab located at the top of the report dialog box.

Summary Media Gateway Link Report

Displays the following aggregate information of all the VoIP sessions for the selected media gateway:

- Jitter
- RTT
- % Loss
- Max Jitter
- Jitter Buffer Overruns
- Jitter Buffer Underruns
- Jitter Buffer Delay
- Max Sequence Jump
- Number Sequence Jumps
- TTL
- Max Sequence Fall
- Number Sequence Falls

The following image is a sample Summary Media Gateway Link report.



To view a Summary Media Gateway Link Report

1. From the System pane, select an object or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.
2. Click **Report**. The Media Gateway Link reports appear.
3. Click the **Summary** tab.

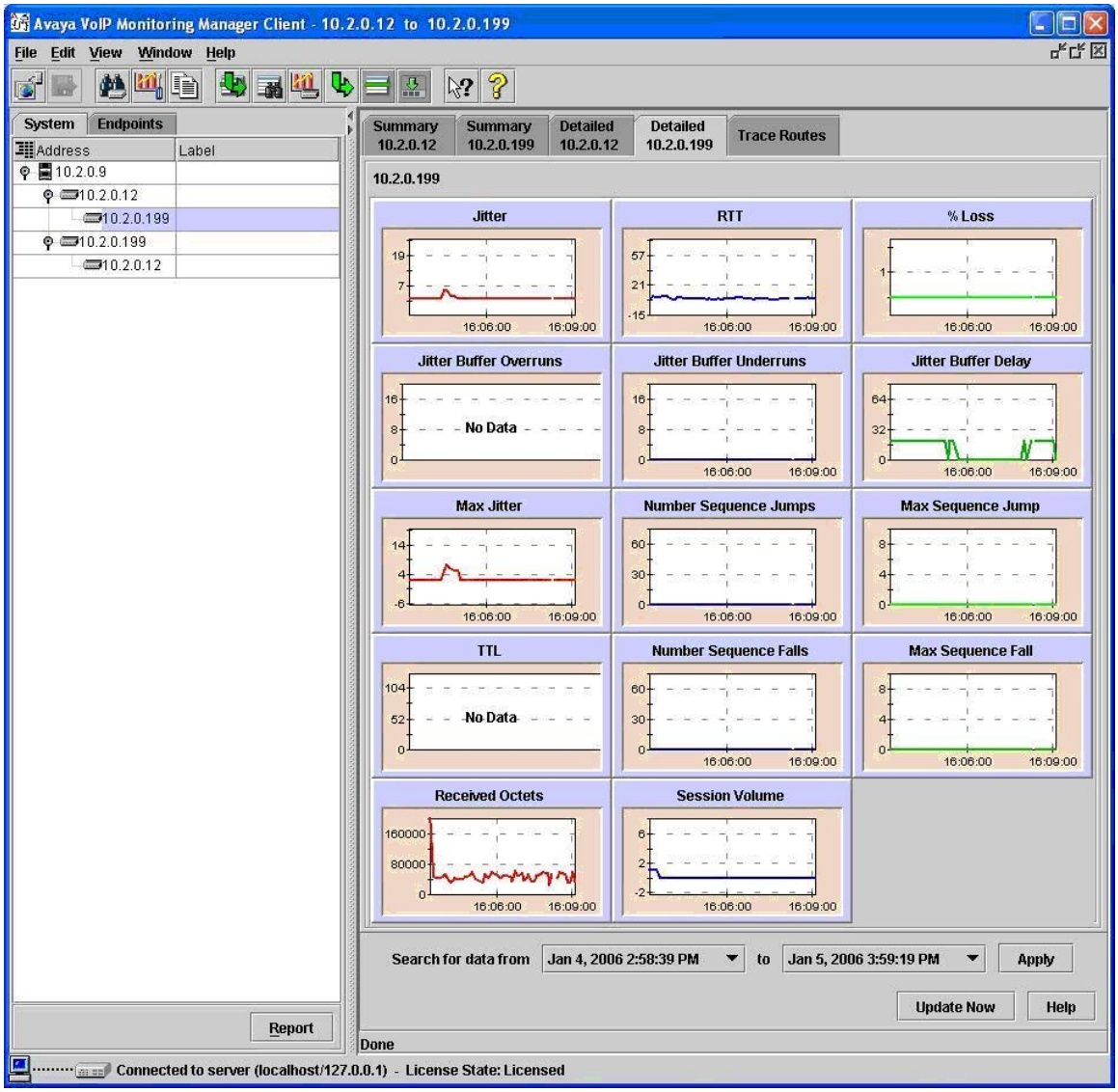
Detailed Media Gateway Link Report

Detailed Media Gateway Link reports display the following aggregate information on graphs for VoIP sessions going between the two selected media gateways:

- Jitter
- RTT
- % Loss
- Jitter Buffer Overruns
- Jitter Buffer Underruns
- Jitter Buffer Delay
- Max Jitter
- Number Sequence Jumps
- Max Sequence Jump
- TTL
- Number Sequence Falls
- Max Sequence Fall
- Received Octets
- Session Volume

This report excludes VoIP sessions at the media gateways that are with phones.

The following image shows a sample Detailed Media Gateway Link report.



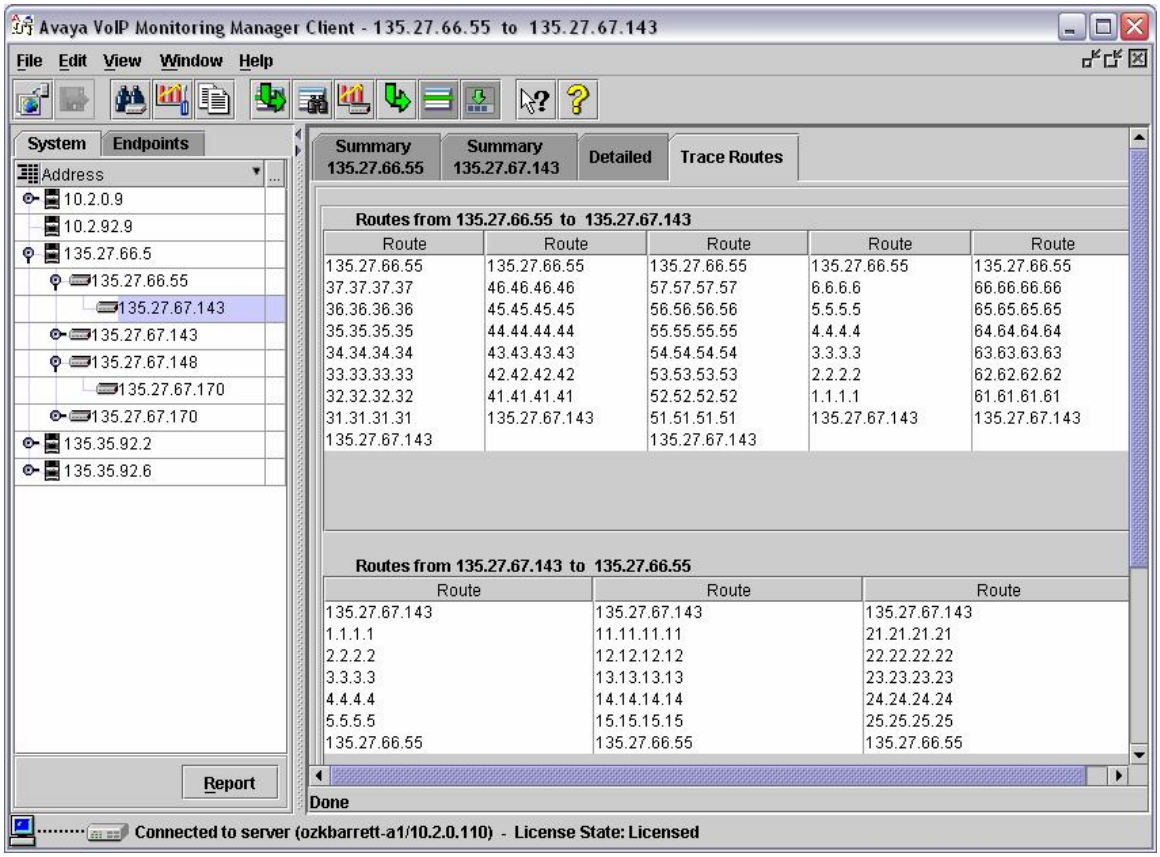
To view a Detailed Media Gateway Link Report

1. From the System pane, select an object or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.
2. Click **Report**. The Media Gateway Link reports appear.
3. Click the **Detailed Report** tab.

Trace Routes Media Gateway Link Report

Shows the probable routes used between the two selected media gateways.

The following image shows a sample Trace Routes Media Gateway Link report.



To view a Trace Routes Media Gateway Link Report

1. From the System pane, select an object or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.
2. Click **Report**. The Media Gateway Link reports appear.
3. Click the **Trace Routes** tab.

View a Report

You can generate reports for endpoints and media gateways.

Endpoint Reports

After you run a search, you can view the report on selected endpoints and endpoints involved in a session. There are two types of Endpoint reports: Summary Reports and Detailed Reports.

To View the QoS Data for an Endpoint

1. From the **Results List,** select an **endpoint** or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.
2. Click **Report**. The Report dialog box opens.

Media Gateway Link Reports

From the System pane, you can select a media gateway and click the **Report** button to view an aggregated report of all the VoIP sessions over the selected link. There are three types of Media Gateway Link reports: Summary Media Gateway Link Report, Detailed Media Gateway Link Report, and Trace Routes Media Gateway Link Report.

Close Report

You can close the report window by performing one of the following steps:

- Click on the **Close** button on the Title Bar of the report.
- Select the **Close** option from the **Window** menu (Ctrl + w, then e). The Close button is the last button on the right hand side of the report. The icon has an X in the middle of it as shown above.

Close All Reports

You can close all the reports simultaneously by selecting the **Close All** option from the **Window** menu. If you only want to close one report, click on the **Close button** on the report.

You can also select **Window > Close** (Ctrl + w, then l).

Copy Report

You can copy the reports to the computer's clipboard. This enables you to paste the report as an image into other applications.

To Copy

1. Click on the title bar of the report you want to copy.
2. Select **Edit > Copy Report** (Ctrl + C).
3. Open the application (such as Microsoft Work or Microsoft Excel) in to which you want to paste the report.
4. Press **Ctrl + v** on your keyboard to paste the report.

If you are using the VoIP Monitoring Manager Web Client then you will be unable to copy the reports to another program.

Move the Reports

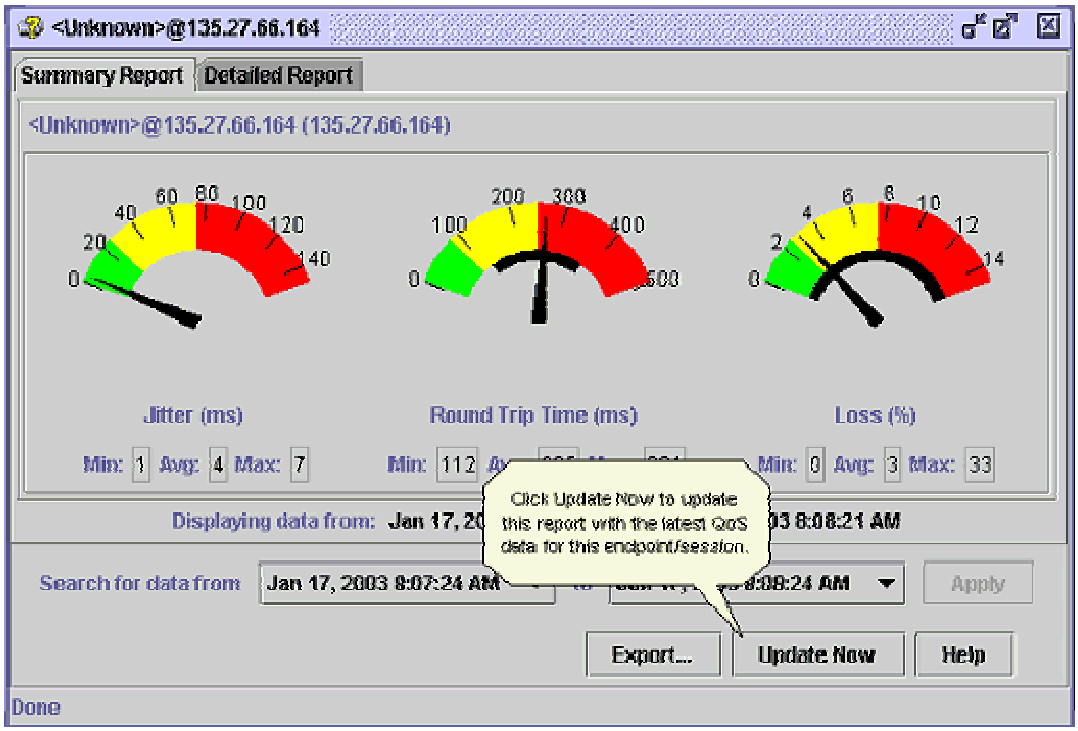
You can drag and drop the reports around the display area to assist with viewing. To move the report, click on the Title Bar with your left mouse button, and by holding the button down, drag the Title Bar across the screen. If you cannot see the Title Bar, you may need to expand the viewing area or use the scroll bars to bring the Title Bar into view.

Expand and Shrink the Reports

You can also expand and shrink a report, by pointing your mouse at the report's borders, when the cursor changes into a bi-directional arrow, hold down your left mouse button and drag the report's borders to the size you want. You can also apply this action to the whole application to make it bigger or smaller.

Update Report

To update an individual report, click on the **Update Now** button located on the Report dialog box. The report will update with the QoS data for the endpoint/session.



Update All Reports

To update all reports that are displaying, click the **Update All Reports** icon. This icon is located on the Tool Bar and the menu option can be accessed from **View > Update All Reports**.

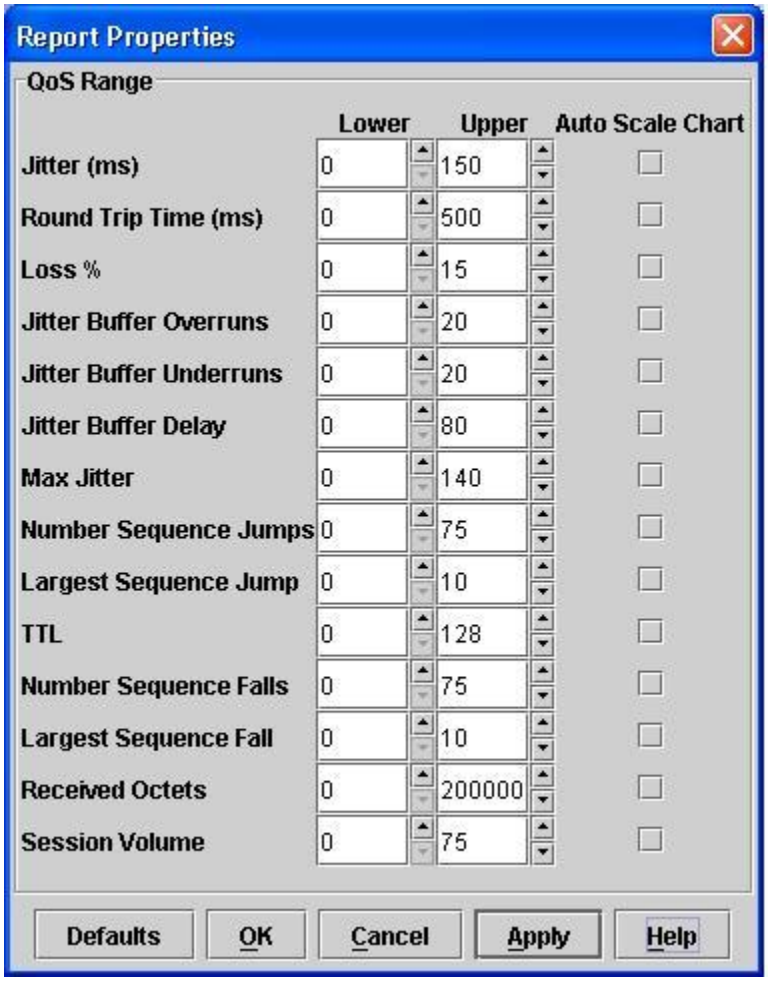
Edit Report Properties

The Report Properties dialog is accessed from the **Edit** menu. It enables you to edit the range of the scale for each of the QoS parameters displayed on the reports.

To alter the range, type in a number in the fields or use the arrow buttons and click **Apply** or **OK** to save your changes.

To reset the parameters to the default settings, click **Defaults**.

To close the dialog without saving any changes, click **Cancel**.



Changing the Date Range of Reports

You can change the date range that appears on an individual report. This enables you to zoom in or out on a time period and see more or less of the detail. If you select a shorter date range, then you will see more data on the graph. If you select a longer date range, then you will see less detail.

Displaying data from: Jul 3, 2002 1:23:10 PM to Jul 9, 2002 3:29:29 PM
Search for data from
Jun 1, 2002 10:04:47 AM
to
Jul 17, 2002 10:04:47 AM
Apply

To Alter the Date Range

1. From the report, click the **Search data from** and the **to** drop-down boxes to access the calendars. You can click on the day and use the arrow buttons to scroll through AM/PM, seconds, minutes, hours, months and years.

2. Click **Apply.** The Report updates with the QoS data for the adjusted date range.

Interpreting Reports

Interpreting the Values Using Detailed Reports

You interpret the Detailed Reports by noting where the sampled QoS data displays on the line graph and noting when this may have occurred. The upper values on the Y-Axis indicate unacceptable limits. The X-Axis shows the date.

Table of Values for Detailed Reports

Jitter (ms)	Round Trip Time (ms)	Loss (%)
> 150ms **Not Acceptable**	**> 500ms** **Not Acceptable**	**> 30%** **Not Acceptable**
50 to 150ms **Warning** Crackling, static or intermittent delay could be reported.	**150 to 500ms** **Warning** Slight pause in the conversation at the lower end of the range to more lengthy delays at the top end of the range could be reported.	**10 to 30%** **Warning** Drop out and missing parts of the conversation could be reported.
0 to 50ms **Acceptable** Conversation was smooth.	**0 to 180ms** **Acceptable** No delay between each endpoint.	**0 to 10%** **Acceptable** No drop out in conversation.

Interpreting the Values Using Summary Reports

You interpret the Summary Reports by noting where the needle on the gauges is positioned for each of the QoS gauges. When the needle is positioned in either the yellow or red ranges, it is indicating degradation in the QoS. The needle on the gauge shows the average values measured and the black inner arc shows the range of values measured. These values also display below each gauge.

Table of Values for Summary Reports of Endpoints

	Jitter (ms)	Round Trip Time (ms)	Loss (%)
	0 to 50ms	**0 to 180ms**	**0 to 10%**
	Acceptable Conversation was smooth.	**Acceptable** No delay between each endpoint.	**Acceptable** No drop out in conversation.
	50 to 150ms	**180 to 500ms**	**10 to 30%**
	Warning Crackling, static or intermittent delay could be reported.	**Warning** Slight pause in the conversation at the lower end of the range to more lengthy delays at the top end of the range could be reported.	**Warning** Drop out and missing parts of the conversation could be reported.
	> 150ms	**> 500ms**	**> 30%**
	Not Acceptable	**Not Acceptable**	**Not Acceptable**

Y-axis

The Y-axis on the Detailed Reports line graphs is the vertical area of the report, covering the top to the bottom of the graph. The top of the Y-axis represents the upper levels for each of the QoS parameters and the bottom of the Y-axis represents the lower levels. You can point your mouse at the samples on the line graph and the exact time and QoS value will display. For more detailed information, see the topic on About Detailed Reports and/or Interpreting Detailed Reports.

Different Scales for Each QoS Parameter

The QoS parameters have different values. To represent each parameter on the same report, the Y-axis has a different scale that suits each QoS parameter. These scales are shown on the Y-axis in their respective colors.

X-axis

The X-axis on the Detailed Reports represents the date range. It is the horizontal area of the line graph, from the left to the right of the report. The start of the date range begins from the left of the horizontal axis and continues until the end of the date range on the far right side.

Alter the Date Range to Show More Detail

You can alter the date range to a shorter date or longer date period to see more or less detail.

Gateway

The Results List will display one or more phone numbers next to the Gateway endpoint type. These phone numbers are the phone numbers for which that the Gateway is acting as an intermediary. Therefore, the phone number of the Gateway can change and can be multiple phone numbers. The Results List will separate endpoints involved in a session with a comma (,). Conferenced calls are separated by a colon (:).

For example, if the following phone number **8616,1111:1222, 8904** displays in the Results List, then the Gateway has three active sessions as explained:

- Telephone 8616 is a non-IP telephone that is in a session with a Softphone.
- Telephones 1111 and 1222 are conferenced (for example, IP phone 8888 is in a session with these two phones).
- Telephone 8904 is a non-IP telephone in a session with an IP telephone.

Arranging Reports

Maximize Reports

You can expand the report to fill the whole viewing area by clicking on the **Maximize** button on the report or from the **Window** menu. The Maximize button is the second button on the report's Title Bar. It is next to the **Close** button. If you select to maximize a report, you can undo maximize from the Window menu.

To maximize reports, select **Window > Maximize** (Alt + w then, m).

Arrange Icons

The Arrange Icons option on the Window menu enables you to line reports up along the bottom of the application. For this option to be available, you must have a report minimized.

To arrange icons, select **Window > Arrange Icons** (Alt + w, then a).

Arrange the Reports on the Screen

You can organize the reports in the VoIP Monitoring Manager display area using the following options from the Window menu. Multiple reports. For more information, click on any of the following options:

- Cascade
- Maximize
- Tile Horizontally
- Tile Vertically
- Arrange Icons
- Close
- Close All

You can also hold your mouse down on the Title Bar of each report and drag the report across the screen or click on the Minimize, Maximize, or Close buttons. To re-open a window that you have minimized, double-click on the minimized Title Bar.

Tile Vertically

You can tile all reports vertically so that each report is lined up, one next to the other showing the Title Bar and the QoS data. If you still have difficulty viewing the reports, try maximizing the application or closing either the **Tool Bar** or **Results List**.

To tile the reports vertically, select **Window > Tile Vertically** (Alt + w, then v).

Tile Horizontally

You can tile all reports horizontally so that each report is lined up, one above the other showing the Title Bar and the QoS data. If you still have difficulty viewing the reports, try maximizing the application or close either the **Tool Bar** or Results List (**View** > **Tool Bar** or **Results List**).

To tile the reports horizontally, select **Window > Tile Horizontally** (Alt + w, then h).

Cascade Reports

You can cascade all the reports so that each report overlaps the other showing the title bar for ease of access.

To cascade the reports, select **Window > Cascade** (Alt + w then c).

Minimize the Reports

You can minimize the report so that only the Title Bar is visible in the viewing area by clicking on the **Minimize** button on the report. The Minimize button is the first button on the report's Title Bar. It is next to the **Maximize** button. To return the report to its normal state, double click on the Title Bar.

View Multiple Reports

You can view multiple reports at one time by repeatedly selecting endpoints and clicking on the **Report** button. You may need to arrange the reports on the screen so that you can see them easily. You can minimize and maximize the reports. If you have minimized a report, you can easily maximize it by double-clicking on its title bar.

View Sessions in a Report

Since a single phone call could include several sessions (for example, if the call was shuffled, conferenced, transferred, and for the initial dial tone), you can view both endpoints involved in the session in a single report. The reports display the parent endpoint involved in the session in the top part with the child endpoint in the bottom part of the report. By displaying in this manner, you can view both endpoints at the same time and compare the QoS information.

To View Sessions in a Report

1. Run a Search. The Results List updates.
2. In the Results List, expand the **parent endpoint** by clicking the icon positioned in the far left column. The child endpoints display in a sub list.
3. Select a **child endpoint**. The Report button becomes available.
4. Click **Report.** A Summary Session Report displays showing the parent endpoint with another report below showing the child endpoint involved in the session. To view the Detailed Session Report, click the **Detailed Report** tab or click the Session Properties tab.

Export Data (Client)

Export Result List

You can export the data in the results list to a comma separated value (csv) file.

The exported data contains records for every endpoint and every session that is displayed in VoIP Monitoring Manager. Opening or closing session folders (to show or hide the endpoints) does not affect the data that is exported.

You can open this file in most database and spreadsheet programs such as Microsoft Excel. Exporting the data to a spreadsheet enables you to manipulate the data so you can create your own reports. Click this link to see an example (Adobe Acrobat 5 or later required – the page has been split into three because of its width). You can use the sorting, counting, and calculation features of Microsoft Excel to create your own reports from this raw data.

The data exported is divided into 3 tables:

- Session Table
- Time-varying Data Table
- Trace Route Table

To Export Data from the Result List

1. Perform one of the following steps:
    - From the File menu, select **Export Result List**.
    - Click the **Export** button located at the bottom of the **Result List**.

    Tip: If you want to limit the data that is exported, narrow down your search so that less data displays in the Result List.
2. In the Save as dialog box, navigate to a folder.
3. In the **File name** box, type a name for the file.
4. Click **Save as**. The file saves with the CSV extension.
5. From Microsoft Excel, open the file. From here you can build your own report.

Microsoft Excel can only handle 65,536 rows of data. If your exported data file contains more rows, you will need to write a script that splits the data into smaller files before you import the data into Excel.

Export Report Data (one session)

You can export the data from a single report to a comma separated value (csv) file by using the **Export** button located on the Report dialog box.

Only the data from the selected report is exported (that is, the data that matches one session, rather than a summary for multiple session).

The recommended spreadsheet is Excel. Exporting the data to Excel enables you to manipulate the data so you can create your own statistical reports. Click this link to see an example (Adobe Acrobat 5 or later required – the page has been split into three because of its width). You can use the sorting, counting, and calculation features of Microsoft Excel to create your own reports from this raw data.

The data exported is divided into 3 tables:

- Session Table
- Time-varying Data Table
- Trace Route Table

To Export Data from the Report Dialog

1. Click the **Report** button located on the **Report** dialog box. A Save dialog box opens.
2. Navigate to a folder.
3. In the **File name:** field, type a name for the file.
4. Click **Save as**. The file saves with the CSV extension.
5. From the spreadsheet program, open the file. From here you can build your own report.

Microsoft Excel only handles 65,536 rows of data. If you need to export more data, you will need to write a script that allows you to export more data or you could try exporting it to a database program such as Access.

Top

Creating Reports with Exported Data

You can export the data from the Result List and/or Report dialog boxes to Microsoft Excel. Using Microsoft Excel you can create your own reports as shown in the linked example. This report was created by using Microsoft Excel's calculation features. It includes averaging results, counting the number of sessions and unique participants, setting filters to determine the longest sessions, and creating a line graph to visually demonstrate the information. You can create your own reports from the exported data. click this link to see an example (Adobe Acrobat reader is required).

Overview of VoIP Monitoring Manager (Server)

VoIP Monitoring Manager Options

The Options dialog box allows you to define and change the Data Storage, RTCP, and Configuration Messaging settings.

The SNMP Configuration dialog box allows you to define and change the SNMP settings.

To Edit VoIP SNMP Settings

1. Select **Edit** > **SNMP Settings** from VoIP Monitoring Manager Server. The SNMP Configuration dialog box displays.
2. Enter a value for SNMP Community ID.

To Edit VoIP Monitoring Manager Options

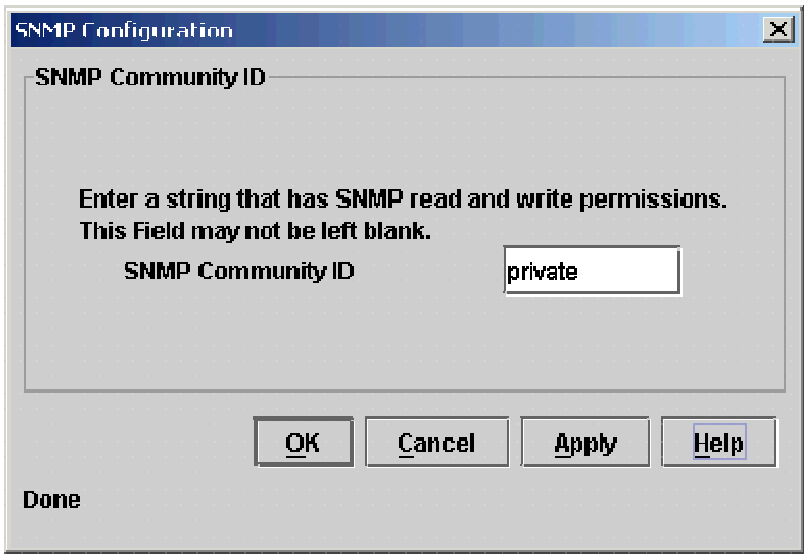
1. Select **Edit** > **Options** from VoIP Monitoring Manager Server. The Server Options dialog box displays.
2. Click the **Data Storage** tab, **RTCP** tab, or the **Configuration Messaging** tab to select settings and type values.

SNMP Settings Dialog Box

The SNMP dialog box contains the Community ID field, which is an RTCP Monitor property as defined for your Windows SNMP Agent. The SNMP dialog box allows you to configure the community IDs to be used so that the server can communicate with the SNMP agent.

> The SNMP Community ID must have read and write privileges. To check this setting or to create other IDs, refer to Check for Valid Community ID.

For more information about the SNMP dialog box, click the Community ID field on the following image.

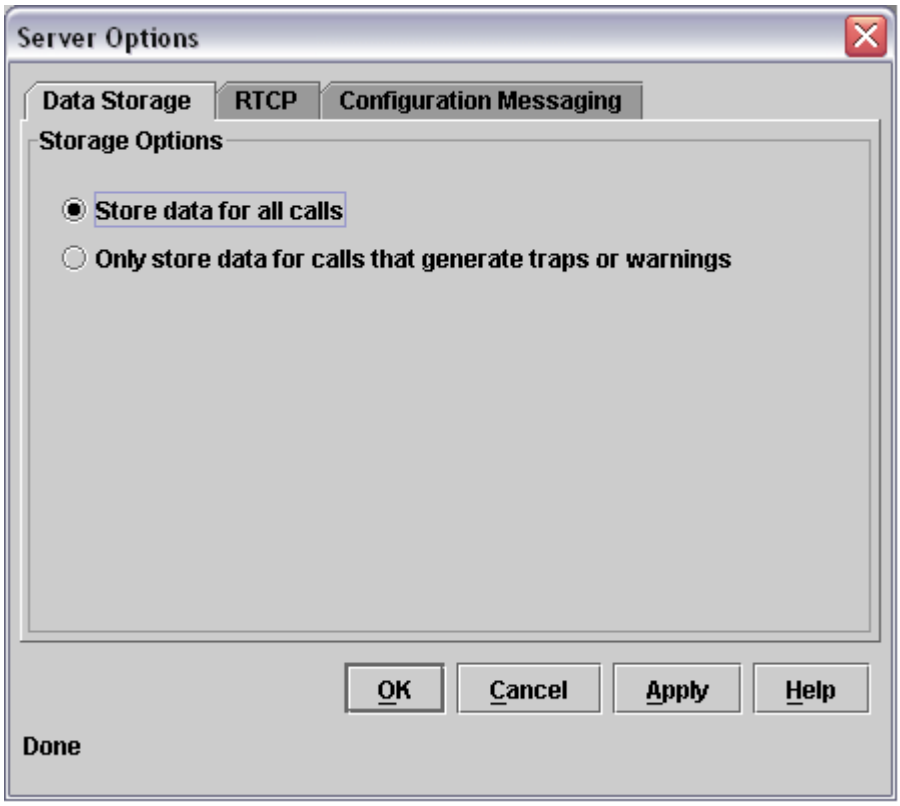


Top

Data Storage Tab

The Data Storage tab allows you to configure data storage options.

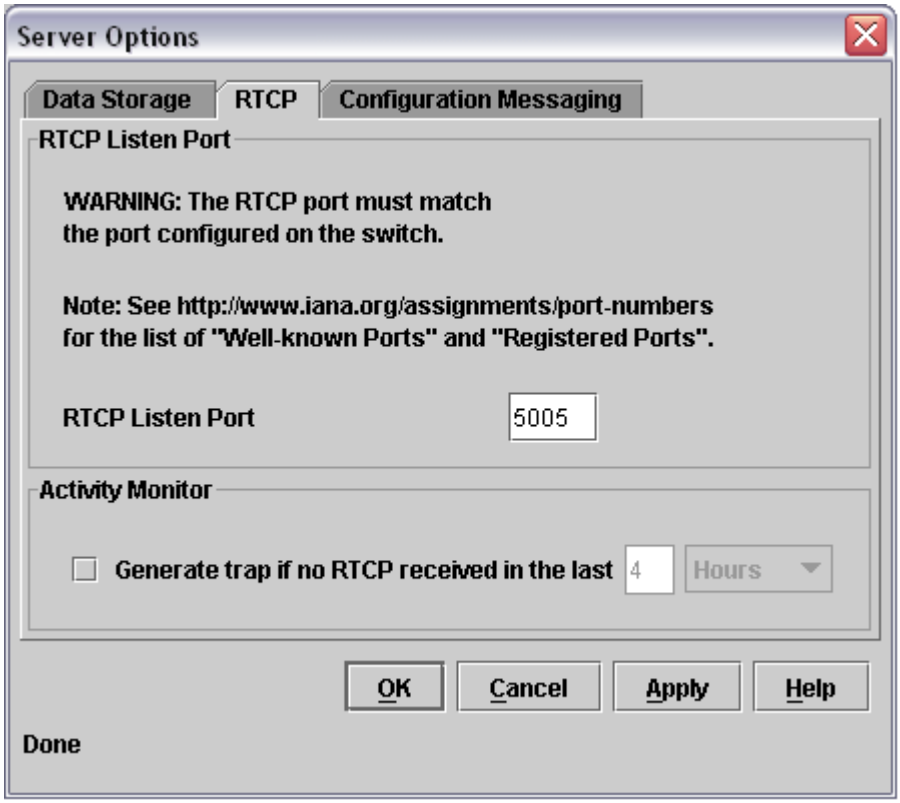
For more information about the Data Storage tab, click the Storage Options area on the following image.



RTCP Tab

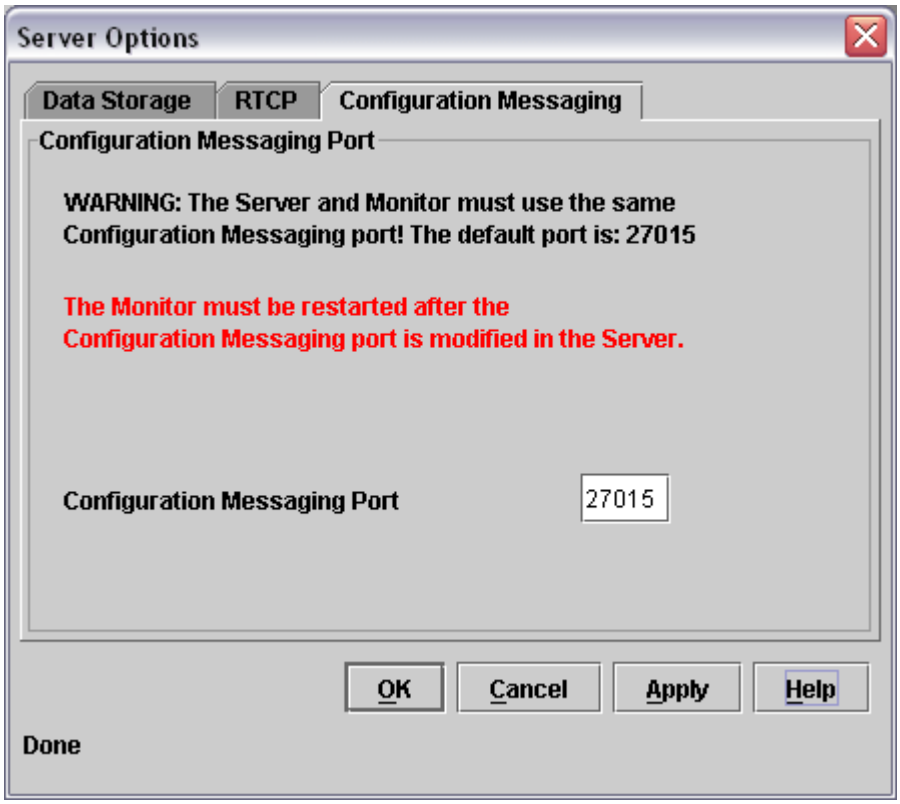
The RTCP tab contains the RTCP Listen Port field that matches the port configured in the Switch Administration Forms (SAT) for the Avaya Communication Manager system. You can also configure the RTCP listen port and generate a trap based on inactivity.

For more information about the RTCP tab, click the Listen Port and Activity Monitor fields on the following image.



Configuration Messaging Tab

The Configuration Messaging tab contain the Configuration Messaging Port field. The server and monitor must use the same Configuration Messaging port.



About RTCP Monitor

The RTCP monitor collects the RTCP packets sent from the Avaya endpoints and stores the information in a proprietary database. The RTCP monitor also runs as a sub-agent of the Windows SNMP agent. All the information contained in the database can be queried through SQL.

The specifications for querying the database are found in:

- The RTP MIB. The reference is located at http://www.ietf.org/rfc/rfc2959.txt
- The proprietary AVAYA-VMON-MIB (The ASN.1 definitions of this MIB and associated traps are included as text files in the installation)

Components of RTT

RTT can comprise the following four components:

- **Propagation delay:** The time it takes for a packet to travel across the network from sender to receiver. This variable is based on the speed of light and the distance the signal must travel. For example, the propagation delay between Singapore and Boston is much longer than the propagation delay between New York and Boston.
- **Transport delay:** The time it takes to traverse the network devices along a transmission path. Networks containing many routers, firewalls, congestion and low-speed WAN services, for example, introduce more delay than an overprovisioned LAN on a single floor of a building.
- **Packetization delay:** The time it takes for a compressor/decompressor (codec) to digitize an analog signal, build frames and then reverse the process at the other end. The G.729 codec has a higher packetization delay than the G.711 codec.
- **Jitter buffer delay:** The delay introduced by the receiver while it holds one or more packets to reduce variations in packet arrival times.

Activity Monitor

Provides the ability to monitor RTCP activity for a set number of minutes, hours, or days. A trap is generated when no activity is received within the specified time period. The number must be from 1 through 99.

The check box is cleared with a setting of 4 hours, as a default setting.

About the Database

By default, all data sent to VoIP Monitoring Manager via RTCP from the endpoints is stored in the database. You can run reports against this data or export it for use in other programs, such as spreadsheets. Depending on the number of monitored terminals and the trap settings, the repository of data can become substantial.

VoIP Monitoring Manager is supplied by default with an MSDE database, which has a maximum size of 2 GB per database. You can migrate to an SQL Server 2000 database or an SQL Server 2005 database.

If you are using an MSDE database, the historical data is stored for 30 days in the database. After 30 days, the data will be deleted.

If you are using an SQL Server 2000 database or an SQL Server 2005 database, the historical data is stored for 100 days in the database. After 100 days, the data will be deleted.

If you need access to historical data, you must either backup the database or export reports that include the required data.

Data Storage Limits and Management

If you are using an MSDE database, the historical data is stored for 30 days in the database. After 30 days, the data will be deleted.

If you are using an SQL Server 2000 database or an SQL Server 2005 database, the historical data is stored for 100 days in the database. After 100 days, the data will be deleted.

Storage Options

Store data for all calls

Records information for all calls identified by Avaya VoIP Monitoring Manager.

Only store data for calls that generate traps or warnings

Records information only for calls where the QoS levels result in a trap or warning as per the traps configurations. When this option is selected, calls are not visible unless a trap has been generated for those calls. Both ends of the session are visible for the duration of the call. If no thresholds have been exceeded for a call, no information will be recorded for that call. This is the default setting in the VoIP Monitoring Manager Server.

Data can still be viewed while a call is active.

License Server Administration Dialog Box

Enables you to log into the WebLM server that manages your Avaya licenses. The license server is required to activate VoIP Monitoring Manager beyond the 90-day trial period. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.

License Server

Enter the IP address of the WebLM server.

Port Number

Enter the port number.

Click the **OK** button to connect to the license server.

If you click the **Cancel** button, you will be able to start VMM, but you will only be able to use it for 90 days. The Status Bar area will indicate that VMM is operating in Evaluation mode and display the number of days remaining.

About Dialog

This dialog box shows

- the version of VMM
- the current license state (that is, whether you are using a valid license or you are running VMM in evaluation mode)
- the number of licenses purchased
- the number of phones at the local server. This number represents the phones that reported to VMM in the last 28 days. This number will increase if you move phones (for example, change extensions or IP addresses). In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, this will not be a problem.
- the number of phones at the local server that exceed the license (that is, the number of phones that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more phones stored in the database than licenses purchased.
- the number of media gateways at the local server. This number represents the media gateways that reported to VMM in the last 28 days.
- the number of media gateways at the local server that exceed the license (that is, the number of media gateways that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more media gateways stored in the database than licenses purchased.

Avaya provides a 90-day trial version of VoIP Monitoring Manager. After 90 days, VoIP Monitoring Manager stops collecting RTCP data. You have the option of purchasing the VoIP Monitoring Manager license key. This key is required to fully activate the VoIP Monitoring Manager beyond the 90-day trial period. When a license key is purchased, an instance of WebLM License Server is required to manage the license key. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.

Getting Started with VoIP Monitoring Manager (Server)

Starting VoIP Monitoring Manager Client

You need to ensure that the VoIP Monitoring Manager (VMM) Server is installed and running on the network before you start the VMM Client. If you only have the VMM Server installed, you can also start the VMM Client as a Web Client.

To start VoIP Monitoring Manager Client:

From the PC where the VoIP Monitoring Manager Client software is installed, select **Start > Programs > Avaya > VoIP Monitoring Manager > Client**.

The Avaya VoIP Monitoring Manager Client window appears. Now you can search for endpoints and then view the QoS data in a report format.

Starting VoIP Monitoring Manager Web Client

The Avaya VoIP Monitoring Manager Client can run as a Web application in a browser. This is useful if you only have the server installed. To run the Avaya VoIP Monitoring Manager Client as a Web application, the following requirements must be met:

- The PC on which the Avaya VoIP Monitoring Manager Server software is installed must be running a Web server. The Apache Web server is automatically installed on the server when the Avaya VoIP Monitoring Manager Server software is installed.
- The Web server must be configured to publish the file to the following VoIP Monitoring Manager installation path:
  C:\Program Files\Avaya\VoIP Monitoring Manager\jars\ClientApplet.htm
- The PC you will use to access the Avaya VoIP Montoring Manager Server must be able to connect to the VMM server via a Web browser and have the following software installed:
  - Microsoft Internet Explorer 6 or later
  - SUN Java 2 Runtime Environment, SE v1.4.2_06

For more information see the topic About the VoIP Monitoring Manager Web Client

To Start Web Client

From your browser, type in the following url:

```
Http://VMMServerMachineName/VoIPMonMgr/ClientApplet.html
```

where VMMServerMachineName = the machine running the VMM Server. This url points to the machine running the VMM Server.

If you do not have the Sun Java Plug-in installed, you are prompted to install it.

To exit the Web Client, just close the browser.

There are limitations in using the VMM Web Client. These are imposed by the security restrictions associated with running unsigned applets. The limitations are:

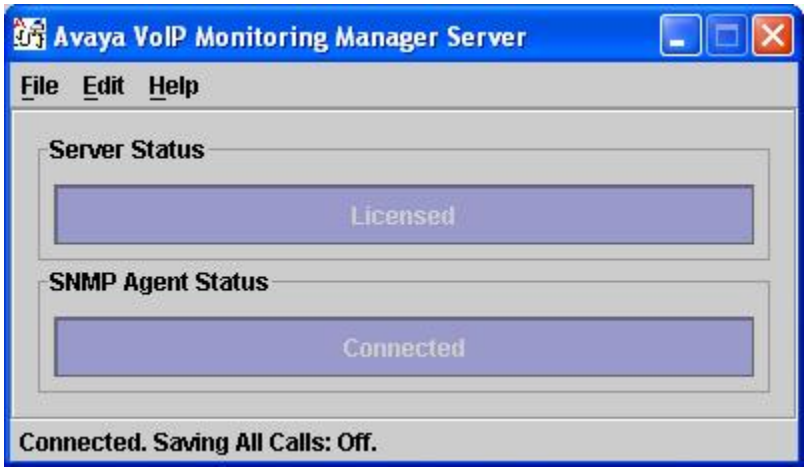
- You can only access one monitor that is directly connected to the server running the VMM Server.
- You cannot:
  - Connect to a new server.
  - Use the Copy functionality.
  - Persist the settings from the Report Properties dialog box.
  - Log to the Windows event log or files.
  - Configure aliases for gateways on the client system.

Monitoring Server Status

When you start the VoIP Monitoring Manager Server, you will see the Server status bar and Windows SNMP Agent status bar. When the Server is running, you will see the **Server Status** bar completely filled in. When the Windows **SNMP Agent** is connected you will also see the SNMP Agent Status bar completely filled in.

From the VoIP Monitoring Manager Server you can:

- Connect to RTCP Monitor
- Edit VoIP Monitoring Manager Options
- Generate Traps
- Configure friendly names for gateways



Connect to RTCP Monitor

The Connect to RTCP Monitor enables you to re-establish the SNMP connection to the RTCP Monitor. When the VMM Server starts, it automatically attempts to establish a connection with the RTCP monitor. If the SNMP connection is lost at any time, select the **Connect to RTCP Monitor** option to try to manually re-establish the connection.

Changing the RTCP Listen Port

The RTCP Listen Port is the configurable port that is used to collect data from the Avaya endpoints. The number must be from 1 through 65535. The default port is 5005.

Changing the RTCP port will result in a warning that the RTCP port must match the port configured on the Avaya voice system. For more information see http://www.iana.org/assignments/port-numbers and your Avaya Call Processing or Switch Administration Forms (SAT).

You will also need to enter a Windows SNMP Agent Community ID with write access. (The default is **private**). It is very unusual to change the listen port since the default of 5005 should work in most situations.

Connecting to the License Server

The Connect to License Server option in the File menu enables you to log into the WebLM server that manages your Avaya licenses. If the license server was not configured during installation, you are prompted to connect to the license server the first time you start the VMM Server.

To connect to the license server:

1. From the File menu, select **Connect to License Server**. The License Server Administration dialog box appears.
2. In the License Server box, enter the IP address of the WebLM server.
3. In the Port Number box, enter the port number.
4. Click the **OK** button.

If you click the **Cancel** button, you will be able to start VMM, but you will only be able to use it for 90 days. The Server Status area will indicate that VMM is operating in Evaluation mode and display the number of days remaining.

Generating Traps & Alarms (Server)

Generating Traps and Alarms

You can set rules to generate traps that notify you when the VoIP network QoS parameters have reached unacceptable levels. You define the rules in the Trap Threshold Settings dialog box, which provides a tab for call traps and a tab for system and terminal traps. To open the Trap Threshold Settings dialog box, select **Edit > Trap Settings** from the VoIP Monitoring Manager Server interface.

You can set more than one rule for each type of trap, and each rule can be made up of more than one condition. When a rule has more than one condition, they must all be satisfied before a trap is sent (that is, they have a logical AND relationship).

The RTCP Monitor generates a trap to a pre-configured Trap Manager when the RTCP Monitor experiences the conditions defined. The Trap Manager is generally configured to be the Gateway Alarm Manager (GAM) or Network Alarm Manager (NAM), but any Trap Manager application can be used. Traps can be set for calls (sessions), systems (networks), and terminals (endpoints).

VoIP Monitor Manager creates traps based on two sets of rules:

- Call Traps. If a specified condition occurs anywhere in the system, a trap is sent immediately.
- System Traps. The specified condition must occur a specified number of times before a trap is sent. This is based on an accumulation of warnings from the entire system.

Recommended Trap Settings

Values that you use to trigger alarms must be fine-tuned to suit your environment. Appropriate settings may vary greatly from one country to another.

The default settings that are in place when VoIP Monitoring Manager is installed are a useful starting point. These settings are based on an environment with high-quality telecommunications facilities. For example, it is reasonable to expect RTT of less than 300.

Severity	Jitter	Delay	% loss
MAJ	60	0	0
MAJ	0	500	0
MAJ	0	0	50
WRN	45	0	0
WRN	0	0	4.0

System warning interval: 100 warnings, 24 hours

Terminal warning interval: 50 warnings, 24 hours

A dialog box with the recommended major alarm settings is shown in Call Traps.

A dialog box with the recommended warning alarm settings is shown in System Traps.

Call Traps

A Call Trap (also referred to as a Call Alarm) is where a trap has been triggered because a customer's call (session) has reached one of the pre-defined QoS parameter's thresholds.

At the end of a call, the RTCP Monitor checks its trap configurations and generates an alarm to a pre-configured Trap Manager. The conditions for the trap are defined in the Trap Threshold Settings dialog box.

The system alarm can be based on any combination of jitter, delay (RTT), or packet loss.

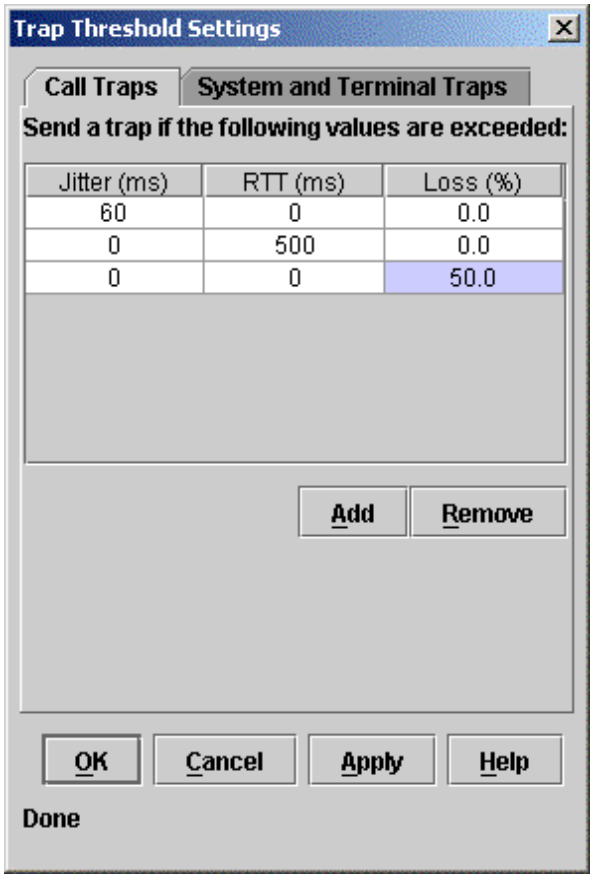
Example

This example shows values entered into the Trap Threshold Settings dialog box. These values would result in a trap being sent at the end of the call if at any time during the call one of the following conditions exist:

- jitter >=60
- delay >= 500
- %loss >= 50

If the conditions in any one line are reached, then the following lines are not read. This is done to ensure that the number of traps sent for a given call is not greater than one.

Click the tabs and columns in the image for more information.



System Traps

A system trap (also called a system alarm) is where a trap/alarm has been triggered because the number of warnings has exceeded the defined threshold. The trap is defined in the Trap Threshold Settings dialog box.

A trap can be defined for the total number of warnings detected on the system, or the total number of warnings detected on an individual terminal. Each trap has a specified interval during which the number of warnings must be accumulated.

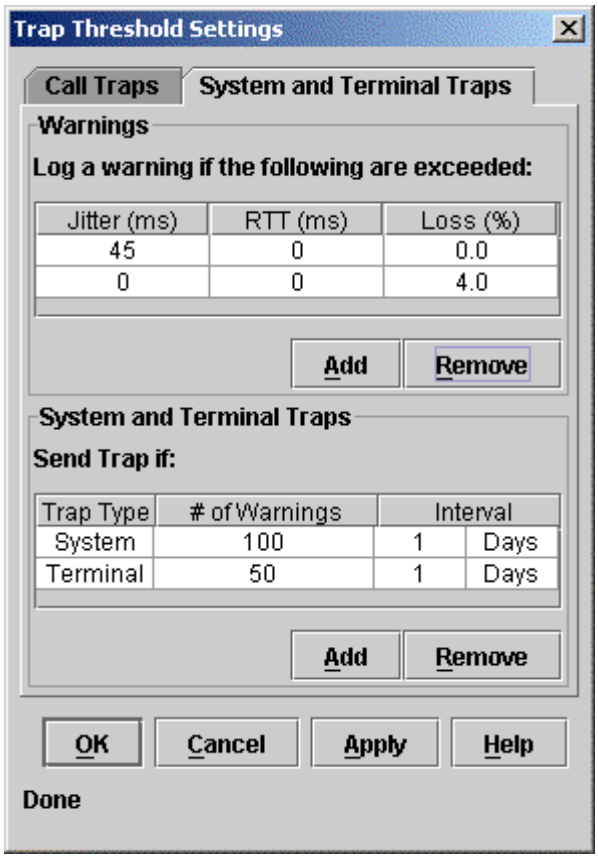
The RTCP Monitor periodically checks to see if the defined interval has expired. It counts the number of warnings recorded during this interval. If it has reached the defined threshold, a system alarm is generated. To generate an alarm as soon as the thresholds are reached, use an interval of zero (0).

The system alarm can be based on any combination of jitter, delay (RTT), or packet loss.

Example

This example shows values entered in the Trap Threshold Settings dialog box. These values would result in a warning being logged at the end of the call, if at any time during the call the jitter >=45, or the %loss >= 4. If the number of warnings logged in any 24-hour period exceeds 100, as defined in the **System's No# of Warnings** column, a system trap is sent.

Click the tabs in the image for more information.



Terminal Traps

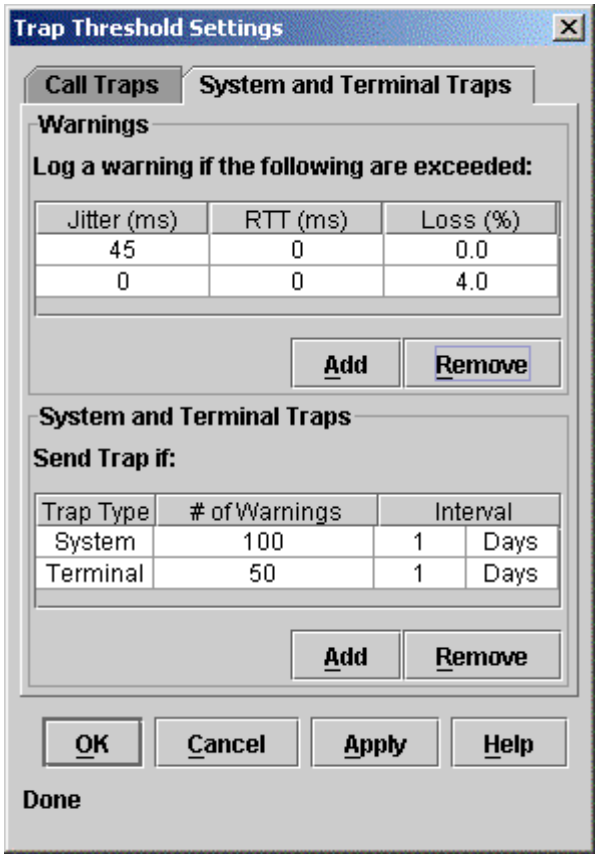
A terminal trap (also called a terminal alarm) is where a trap has been triggered because the number of warnings for any one terminal (endpoint) has exceeded the defined threshold. The trap is defined in the Trap Threshold Settings dialog box. You can set traps for each of the QoS parameters for calls (sessions), as well as thresholds for systems (networks), and terminals (endpoint) in the Trap dialog box.

The RTCP Monitor checks to see when the defined interval expires. It counts the number of warning traps for a specific IP endpoint. A terminal trap is sent when the number exceeds the specified number in the defined interval. To generate an alarm as soon as the thresholds are reached, use an interval of zero (0).

Example

This example shows values entered into the Trap Threshold Settings dialog. These values would result in a warning being logged at the end of the call, if at any time during the call the jitter >=45, or the %loss >= 4. If the number of warnings logged in any 24-hour interval, against a single endpoint (IP Address) exceeds 50, a terminal trap is sent for that endpoint.

Click on the tabs or columns in this example to see more explanations.



Troubleshooting

Troubleshooting

Use this section to look for solutions to common problems.

License Problems

If the About dialog box indicates that you have exceeded the number of licenses, the following conditions may have occurred:

- You moved phones (for example, changed extensions or IP addresses). Moving phones will increase the number of used licenses. In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, and the endpoint count consists of the last 28 days, this will not be a problem.
- You need to purchase additional VMM licenses. Contact your authorized Avaya Sales Representative.

Each VMM RTCP monitor periodically checks the number of endpoints it knows about and requests/renews the licenses for them. If there is more than one RTCP monitor and the total number of endpoints known exceeds the number of licenses, the RTCP monitor that requests licenses first will get its licenses. The RTCP monitor that requests licenses last will be denied licenses. If you enter the 30-day grace period because license limits were exceeded, the About dialog box will appear every time the VMM Server and VMM Client are started. If you exceed the 30-day grace period, VoIP Monitoring Manager stops collecting RTCP data.

Client Error Messages

Client Error Messages

This topic lists some common Client error messages that may occur as a result of mis-configuration or incorrect usage.

Access Error

If you receive the following error message you will need to change the java.policy file using the policy tool provided by SUN. The java.policy file is located in the directory where you installed Avaya VoIP Monitoring Manager. Experienced Administrators should only make changes to this file.

This VoIP Monitoring Manager Client is not permitted to access hostname. Please update the java.policy file to give this client the necessary permission you will need to restart the client or select another host.

Graph Limit Reached

If you receive the following error message, the number of reports opened has reached the VoIP Monitoring Manager's limit. Only ten reports can be displayed at once. You will need to close some reports.

The reports for the selected endpoints could not be displayed, as the limit on the number of reports displayed would be exceeded. Please close some reports, or select fewer endpoints and try again.

Help Could Not Be Displayed

If you receive the following error message, there are problems displaying the help. You may need to check if the VoIP Monitoring Manager is installed correctly.

The help could not be displayed. Please check that the VoIP Monitoring Manager is installed correctly.

Invalid Bounds

If you receive any of the following error messages then the values entered in the Report Properties dialog box is not a valid entry. Check that the value in the left field is less than the value in the right field or in the case for the packet loss field, the value must not be greater than or equal to 100.

> The upper/lower bound must be greater than the lower bound.
>
> The percentage loss upper bound must be greater than the lower bound and less than or equal to **100.**

Invalid Date Range

If you receive this error message then the start date selected in the Search dialog box is after the end date. You will need to change the start date or end date in the Search dialog so that the start date is before the end date.

> The date range is invalid. Please ensure the start date is before the end date and try again.

Invalid Search Parameter

The **Invalid Search Parameter** error message displays if you have entered an incorrectly formatted entry in one or more of the fields in the Search dialog box. Follow the suggested examples in the dialog box. For more information on correct formatting, see the following topics:

- Search for a Specific Phone Number
- Search for a Specify SIP Username
- Search for a Specific Network Address
- Search Using QoS Values

No Data is Displaying on a Report

There are many reasons why data may not display on the report.

Possible Solutions

- If you are using MSDE, data older than 30 days is removed from the database.
- If you are using SQL server, data older than 100 days is removed from the database.
- Check the VoIP Monitoring Manager Options. You may have an incorrect Windows SNMP Agent Community ID or RTCP Listen Port setting.

No Endpoint Data Available

If you receive the following error message, the endpoint whose report is being viewed is not currently active. Wait until the endpoint becomes active again and more data will be displayed, or close the report if you are finished viewing it.

There is no data currently available for this endpoint.

Explanation

This happens when calls are too short to produce reporting data, or the reporting data has been lost.

If the actual call duration is comparable to the reporting period (or shorter than the reporting period), there may be no RTCP packets received. The endpoints normally provide a *reception report*, but in this situation none will be received before the call ends.

Endpoints are identified by data that they send in RTCP packets. Hence if no packet is received, at least one of the session participants cannot be identified. The report shows *unknown endpoint*.

Calls that do not generate one or more RTCP packets are reported as having the default duration of five seconds. The actual call may have been longer – up to 10 or 15 seconds.

Even if one RTCP packet is generated during a short call, it could be lost due to other environmental factors. For example, one participant might have silence suppression enabled, with the packet sent during the suppression period.

No Endpoints Matched the Search

If you receive the following error message, it could be due to one of the situations as described:

No endpoint matched the given search.

- There are no endpoints reporting to the RTCP Monitor or the chosen VoIP Monitoring Manager Server.
- The calls are active, but since no data is being sent to the RTCP Monitor, the ip-network-region form and the system-parameters ip-options form for the Avaya Communication Manager system are not configured correctly.
- There were no endpoints that matched the QoS parameters in the search.
- There were no endpoints that matched the search for phone number, SIP username, Network Address, or date range as specified in the Search dialog box.

Try Broadening the Search:

- Select a different date range in the Search dialog box.
- Use a more general phone number pattern.
- Search for all endpoints instead of just those matching a given phone number, SIP username, or network address.

Server Unavailable

If you receive one of the following error messages, the VoIP Monitoring Manager Server has not been started. You must start the VoIP Monitoring Manager Server and verify that the machine you have attempted to connect with is the machine running the VoIP Monitoring Manager Server. If you are using the Web Client, you must refresh your browser to reconnect to the Server.

Not connected to VoIP Monitoring Manager Server.

The VoIP Monitoring Manager Server on [computer name inserted] is not currently available. Please ensure the server is running and try connecting again.

If you are running the Web Client, the error message will be slightly different as follows:

The Avaya VoIP Monitoring Manager Server is not currently available. Please ensure the server is running and refresh this page in your browser.

For this situation, check the server is running and refresh the browser page (F5 on your keyboard will refresh for most browsers).

Server Version Error

If you receive the following error message, you will need to ensure that the VoIP Monitoring Manager Server is running the same version as the VoIP Monitoring Manager Client.

The VoIP Monitoring Manager Server on [computer name inserted] is running an incompatible version. Please select a compatible Server or upgrade the Client and/or Server.

Try

- Check the Host Name Server dialog box.
- Check that the version number for the Client is the same for the Server.
- From the Client, **Help > About menu**.
- From the Server interface, click **Help > About menu**. If the version numbers are not the same, you will need to close all browsers and download the correct Server version.

If you are running the Web Client, the error message will be slightly different as follows:

The VoIP Monitoring Manager Server is an incompatible version. Please close all your browsers and try again.

For this situation, close all browsers, and then retry using the Web Client. The correct Web Client will automatically download from the server.

Some Fields Are Blank in the Exported Data

Some fields are blank in the exported data because the endpoints did not report the data.

Unknown Error

If you receive the following error message, it is important that you contact customer support so that they can help you and the error can be fixed.

An unknown error occurred. Please contact customer support if this error continues.

Web Client Displaying Incorrect Time

The Web Client will display an incorrect time if you have the JRE 1.4.01 installed. It is recommended that you use the Sun JRE 1.4.2_06 that is supplied with the VoIP Monitoring Manager installation.

Windows SNMP Agent Connection Error

If you receive the following error message, VoIP Monitoring Manager Server is not connected to the Windows SNMP Agent. If you were viewing a report, you will need to open another report or run a search. You may also need to check that the Windows SNMP Agent is installed and running on the VoIP Monitoring Manager or check that the VoIP Monitoring Manager Options has a correct SNMP Community ID.

The server could not reconnect to the SNMP Agent. This server will not be able to retrieve data until this issue is resolved. Try doing another search to make the server try to reconnect to the SNMP Agent, or connect to another server.

Server Error Messages

Server Error Messages

This part of help lists some common Server error messages that may occur as a result of mis-configuration or incorrect usage.

Check SNMP Installation

The Simple Network Management Protocol (SNMP) Agent is the Windows SNMP service that runs on your computer. SNMP is a protocol for communications between remote network management stations and managed network elements (such as Avaya devices).

The VoIP Monitoring Manager Server needs the Windows SNMP Agent installed because it enables the RTCP Monitor to collect and publish the data. The Windows SNMP service is provided with the Windows CD but is not installed by default. You will be prompted during the VoIP Monitoring Manager install to install it from the Windows CD if Windows SNMP service is not installed already.

Could Not Resolve Host Name

If you receive the following error message, the machine running the VoIP Monitoring Manager Server is not correctly configured for TCP/IP. If your IT department cannot resolve this problem, please contact customer support.

`Error starting Server [text of exception raised inserted] Server exiting.`

Excessive Packet Loss

Packet Loss is the result of packets being lost in the transmission from one endpoint to another. When packet loss occurs there could be a drop out of words or partial words in the conversation. At low levels, poor voice quality would result. At high levels, the conversation becomes unintelligible. Packet Loss can result from line congestion.

General Server Error

If you receive the following error message, you must perform one of the following steps:

- Reboot the machine, and restart the VoIP Monitoring Manager Server.
- Contact customer support.

Unknown error starting server. Try rebooting. Please contact customer support if this error continues. Server exiting.

Invalid RTCP Port

If you receive the following error messages then the number entered in the RTCP Listen Port field in the VoIP Monitoring Manager Options is not valid. Enter a number in the range of 1 – 65535.

Please enter a port in the range 1 to 65535.

Ports used by Server

The following ports are used:

Port	Function
161	SNMP Service listens on this port
162	SNMP Trap service listens on this port. Required on the machine running the trap collector (if you are collecting traps).
1099	RMI registry runs on this port
5005	RTCP Listen port. Endpoints send RTCP to the VMM server on this port. If any of the IP endpoints are on the other side of a firewall from the VMM server, the firewall needs to be configured to let these packets through.

Problems Binding to Port 162

When installing the VoIP Monitoring Manager, the Windows SNMP Service and the Windows SNMP Trap Service are also installed. As the Windows SNMP Trap Service opens Port 162, it is possible that it is bound to it. The Windows SNMP Service is required by the VoIP Monitoring Manager to run the RTCP Monitor, but the Windows SNMP Trap service is not required. To prevent the Trap Service from starting automatically and therefore binding to Port 162, set the Trap Service properties to manual at startup.

To Set the Trap Service Startup to Manual

1. From Windows select **Start > Settings > Control Panel**.
2. Double-click **Administrative Tools** to open it.
3. Double-click **Services** shortcut to open it.
4. From Services, scroll down to **SNMP Trap Service** to select it.
5. Right-click **SNMP Trap Services**, and select **Properties.**
6. From SNMP Trap Services Properties dialog, click **Stop.**
7. Select **Startup** drop-down arrow, and select **Manual**.
8. Click **OK** and close all open folders.

RMI Registry Error

If you receive any of the following error messages, the VoIP Monitoring Manager Server is unable to start. You must reboot the machine running the VoIP Monitoring Manager Server.

Problem with RMI Registry. Ensure that port 1099 is available. You can do this by rebooting server PC. Server exiting...

Unknown problem with RMI Registry. Try rebooting. Please contact customer support if this error continues. Server exiting…

Set RTCP Port Error

If you receive the following error message, there is a problem setting the RTCP port. You need to consider checking the following as indicated on the error message:

Setting the RTCP Port failed.

Please check:

The SNMP community ID has write access

The SNMP Agent is running

The port is not in use by another application

Server Cannot Connect to SNMP

This condition is not apparent unless you view the Windows Event Viewer on the server. On a client, it will not be possible to generate reports, but no relevant information is available in the event log.

This condition is caused by incomplete or incorrect installation of the server. The following DLL files cannot be found in c:\WINNT\System32\:

Msvcp70.dll

Msvcr70.dll

Mfc70.dll

To verify that this condition has occurred, look in the System Log section of the Windows Event Viewer for event ID 1102 with the following message:

> SNMP Service is ignoring Extension Agent DLL <path and file name> because it is missing or misconfigured.

If you verify this problem, copy the required DLL files from the installation CD to the required directory.

Correct operation

If the service starts normally, the following information is displayed in Application section of the Window Event Viewer:

- Informational event with ID 500: You are using *RtpMib.dll version 3.1.x*

  (the text shown in italics in this message may vary depending on the version of VoIP Monitoring Manager that is installed.)

- Event Properties with Event ID 500: The Avaya RTCP Monitor has started successfully.

SNMP Service Error

If you receive any of the following error messages, it is possible that the Windows SNMP Agent is not running, or an incorrect SNMP Community ID or an ID without read access is being used. You can restart the VoIP Monitoring Manager Server.

Could not communicate with the SNMP Agent. Please ensure the Agent is running and that the correct Community ID is being used. If further problems are encountered, try running the VoIP Monitoring Manager Server installation again.

SNMP problem encountered. This probably indicates that the SNMP Agent part of the VoIP Monitoring Manager Server installation is corrupted. Please re-run the VoIP Monitoring Manager Server installation again. The VoIP Monitoring Manager Server cannot function correctly until this is fixed. Server exiting...

Unable to establish database connection

This message is displayed when you make an unsuccessful attempt to connect VoIP Monitoring Manager server to a database. Any of the following conditions can cause this error to be displayed:

- The database server name is incorrect (or the IP address is incorrect), or is not accessible on your network.
- The ID is incorrect for the database.
- The password is not correct.

The full message is:

> **Unable to establish database connection(s) using specified credentials. Please check the database server name, user name and password.**

Windows SNMP Agent is Not Running

If you receive this error message, you will need to check that the SNMP Service is installed and running.

Windows SNMP Agent is Not Running

Reference Information

Characteristics of RTCP

Error data is derived from RTCP as follows:

- RTCP provides support for real-time conferencing for large groups within an Internet, including source identification and support for media gateways (like audio and video bridges) and multicast-to-unicast translators.
- RTCP provides information about Round Trip Time, Jitter, Packet Loss, and other data useful for analyzing voice quality.
- Endpoints transmitting real-time data send an RTP stream, which carries the actual data (for example, audio and/or video). The endpoints also send a corresponding RTCP stream. For more information, see RFC 1889 located at http://www.ietf.org/rfc/rfc1889.txt.

Database Schema

```
/**
* Create the Vmm schema.
*/
USE Vmm
GO


/** Drop the Participant table if it already exists. */
IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'Participant')
    DROP TABLE Participant
GO


/** Create the Participant table. */
CREATE TABLE Participant
(
    ID                          uniqueidentifier not null PRIMARY KEY, /* The unique ID
of the session participant. */
    StartTime                   DateTime,               /* Date and time of the first
report received. */
    EndTime                     DateTime,               /* The time the session
finishes. */
    SSRC                        bigint,                 /* Synchronization source
identifier. */
    PeerSSRC                    bigint,                 /* Synchronization source
identifier of the peer. */
    IPAddress1                  tinyint,                /* IP Address of the participant
for this session (Octect 1). */
    IPAddress2                  tinyint,                /* IP Address of the participant
for this session (Octect 2). */
    IPAddress3                  tinyint,                /* IP Address of the participant
for this session (Octect 3). */
    IPAddress4                  tinyint,                /* IP Address of the participant
for this session (Octect 4). */
    RTPIncomingPortFrom         int,                    /* Port on remote machine from
which the RTP stream is being received. */
```

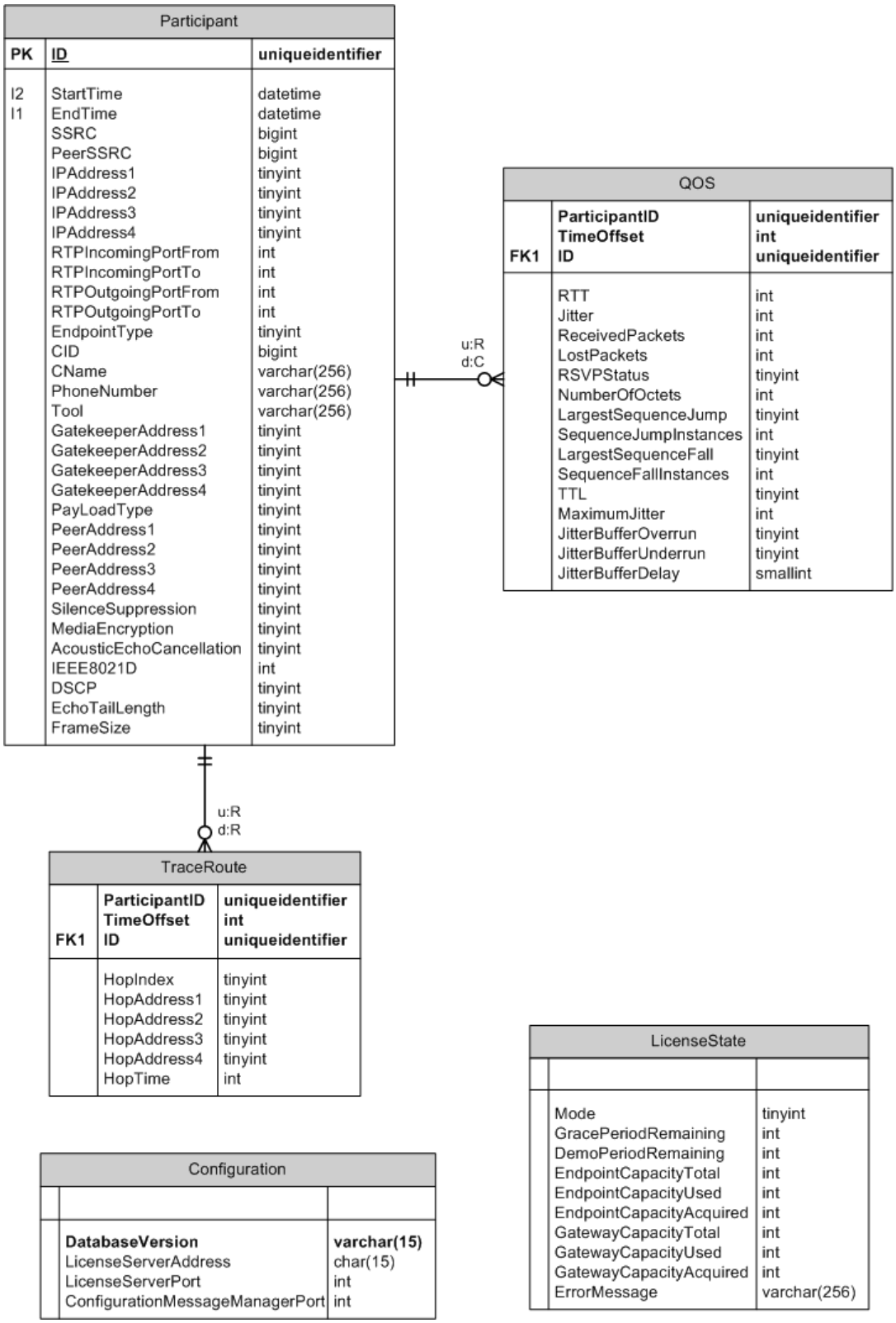
```
    RTPIncomingPortTo           int,                /* Port on local machine from
which the RTP stream is being sent. */

    RTPOutgoingPortFrom         int,                /* Port on local machine from
which the RTP stream is being sent. */

    RTPOutgoingPortTo           int,                /* Port on remote machine from
which the RTP stream is being received. */

    EndpointType                tinyint,            /* The type of endpoint. */

    CID                         bigint,             /* Unique call identifier. */

    CName                       varchar(256),       /* The RTP canonical name of the
participant. */

    PhoneNumber                 varchar(256),       /* Phone number of this
participant from phone SDES item */

    Tool                        varchar(256),       /* The TOOL from the TOOL RTCP
SDES item */

    GatekeeperAddress1          tinyint,            /* The gatekeeper address for
this participant (Octect 1). */

    GatekeeperAddress2          tinyint,            /* The gatekeeper address for
this participant (Octect 2). */

    GatekeeperAddress3          tinyint,            /* The gatekeeper address for
this participant (Octect 3). */

    GatekeeperAddress4          tinyint,            /* The gatekeeper address for
this participant (Octect 4). */

    PayLoadType                 tinyint,            /* Payload type of received
packets. */

    PeerAddress1                tinyint,            /* IP address of peer endpoint
(Octect 1). */

    PeerAddress2                tinyint,            /* IP address of peer endpoint
(Octect 2). */

    PeerAddress3                tinyint,            /* IP address of peer endpoint
(Octect 3). */

    PeerAddress4                tinyint,            /* IP address of peer endpoint
(Octect 4). */

    SilenceSuppression          tinyint,            /* The Silence suppression
metric. */

    MediaEncryption             tinyint,            /* The Silence suppression
metric. */

    AcousticEchoCancellation    tinyint,            /* The acoustic echo
cancellation metric. */

    IEEE8021D                   int,                /* The 802.1D metric. */

    DSCP                        tinyint,            /* The DiffServ Code Point
(DSCP) metric. */

    EchoTailLength              tinyint,            /* The echo tail length metric.
*/

    FrameSize                   tinyint             /* The frame size metric. */

)

GO


/** Create the Participant table indexes. */

CREATE NONCLUSTERED INDEX StartDateIndex ON Participant (StartTime)

GO


CREATE NONCLUSTERED INDEX EndDateIndex ON Participant (EndTime)

GO
```

```
/** Drop the QOS table if it already exists. */
IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'QOS')
    DROP TABLE QOS
GO

/** Create the QOS table. */
CREATE TABLE QOS
(
    ParticipantID               uniqueidentifier not null, /* Participant ID that this
QoS data applies to. */
    TimeOffset                  int not null,   /* Time of the QoS entry from session
start. */
    RTT                         int,            /* Round trip time. */
    Jitter                      int,            /* Jitter. */
    ReceivedPackets             int,            /* Count of RTP packets received since
the last time an RTCP packet was received. */
    LostPackets                 int,            /* A count of RTP packets since the last
time an RTCP packet was received. */
    RSVPStatus                  tinyint,        /* The RSVP status metric. */
    NumberOfOctets              int,            /* The Received RTP Octets metric. */
    LargestSequenceJump         tinyint,        /* The Largest sequence jump metric. */
    SequenceJumpInstances       int,            /* The number of sequence jump instances
metric. */
    LargestSequenceFall         tinyint,        /* The Largest Sequence Fall metric. */
    SequenceFallInstances       int,            /* The number of sequence fall instances
metric. */
    TTL                         tinyint,        /* The Time To Live metric. */
    MaximumJitter               int,            /* The Maximum Jitter metric. */
    JitterBufferOverrun         tinyint,        /* The number of jitter buffer over-runs
metric. */
    JitterBufferUnderrun        tinyint,        /* The number of jitter buffer under-
runs metric. */
    JitterBufferDelay           smallint        /* The Jitter Buffer Delay metric. */
)

/** Create the QOS table indexes. */
CREATE CLUSTERED INDEX ParticipantID ON QOS (ParticipantID, TimeOffset)
GO

/** Drop the TraceRoute table if it already exists. */
IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'TraceRoute')
    DROP TABLE TraceRoute
GO

/** Create the TraceRoute table. */
CREATE TABLE TraceRoute
(
```

```
    ParticipantID       uniqueidentifier not null,  /* The participant ID for which the
QOS samples are recorded. */
    TimeOffset          int not null,               /* Time offset of the trace route
from the session start. */
    HopIndex            tinyint,                    /* Hop count index. */
    HopAddress1         tinyint,                    /* IP Address for the network hop
(Octect 1). */
    HopAddress2         tinyint,                    /* IP Address for the network hop
(Octect 2). */
    HopAddress3         tinyint,                    /* IP Address for the network hop
(Octect 3). */
    HopAddress4         tinyint,                    /* IP Address for the network hop
(Octect 4). */
    HopTime             int                         /* Round trip delay to the hop
address in milliseconds. */
)

/** Create the TraceRoute table indexes. */
CREATE CLUSTERED INDEX ParticipantID ON TraceRoute (ParticipantID)
GO

/** Drop the Configuration table if it already exists. */
IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'Configuration')
    DROP TABLE Configuration
GO

/** Create the Configuration table. */
CREATE TABLE Configuration
(
    DatabaseVersion                     varchar(15),        /* Database version number.
*/
    LicenseServerAddress                char(15),           /* Address of the WebLM
license server. */
    LicenseServerPort                   int,                /* Port of the WebLM license
server. */
    ConfigurationMessageManagerPort     int                 /* The config message
manager port. */
)

/** Add a row to the configuration table with the database version in it. */
INSERT INTO Configuration VALUES('3.1.0', NULL, NULL, NULL);

/** Drop the LicenseState table if it already exists. */
IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'LicenseState')
    DROP TABLE LicenseState
GO

/** Create the LicenseState table. */
CREATE TABLE LicenseState
```

```
(
    Mode                            tinyint,        /* The licensing mode of the monitor
                                                       null = Unknown Mode
                                                       0    = Normal Mode
                                                       1    = Demo Mode
                                                       2    = Restricted Mode */
    GracePeriodRemaining            int,            /* The number of grace period days
remaining */
    DemoPeriodRemaining             int,            /* The number of demo days remaining
*/
    EndpointCapacityTotal           int,            /* The total number of endpoints
licensed */
    EndpointCapacityUsed            int,            /* The number of endpoints currently
active */
    EndpointCapacityAcquired        int,            /* The number of endpoint licenses
currently acquired by the VMM monitor using this database */
    GatewayCapacityTotal            int,            /* The total number of gateways
licensed */
    GatewayCapacityUsed             int,            /* The number of gatways currently
active */
    GatewayCapacityAcquired         int,            /* The number of gateway licenses
currently acquired by the VMM monitor using this database */
    ErrorMessage                    varchar(256)    /* Optional error message associated
with the current license state */
)
```

Entity Relationship Diagram



Handling Jitter

Removing Jitter

Jitter can result from bad queuing strategies set up on network equipment. Check your equipment manual for recommended settings. To remove jitter, the endpoints need to collect packets and hold them long enough to allow the slowest packets to arrive, allowing them to be played at even intervals in the correct sequence, which causes additional delay.

Jitter Effects

Jitter can create audible voice-quality problems if the variation is greater than 60ms. Symptoms of excessive jitter could be reported as crackling or static. A faulty microphone or other hardware problems can be reported as a similar sound problem to jitter, but they are not related. You need to rule out that this is not the cause of the problem.

Interpreting RSVP Status

The RSVP status can change during a session. For example, if the RSVP status for a single endpoint in a session has changed between significant states (such as Failed and Success), VoIP Monitoring Manager will use the label **Various** to represent this situation. However, if the status has only changed from Pending to Success, then VoIP Monitoring Manager will report Success. Also, the RSVP status can be different for each endpoint in the session. For example, RSVP may be disabled for one endpoint in the session, and enabled for the other.

The RSVP status can be:

Unknown:	Information about the RSVP status was not available.
Disabled:	The end-point has been configured to ignore RSVP signaling.
Not in Use:	RSVP is enabled for use but there is no receiver RTP channel session active, or no attempt has been made by the sender to protect the receiver's RTP channel (i.e. no Path message has been received).
Reservation Pending:	This state indicates that the receiver has responded to the first Path message it has received since the call started with a Resv message, and is waiting for a ResvConf to confirm the reservation is installed.
Reservation Failed:	This state indicates that the receiver has had a reservation fail or timeout, or an existing reservation was torn down prematurely.
Reservation Success:	This state shows that the receiver's receiving RTP channel is protected by an installed RSVP reservation. Ideally this reservation will need to be successfully refreshed until the RTP session ends.
Various:	The RSVP status for a single endpoint in a session has changed between significant states (such as Failed and Success).

Interpreting Terminal Names

The canonical name or CNAME is the unique identifier for each participant within one RTP session or set of related RTP sessions.

The format is **user@host,** or **host** if a user name is not available as on single-user systems. For both formats, **host** is either the fully qualified domain name or IP address of the host from which the real-time data originates.

For Avaya VoIP systems CNAMEs are of the format:

IP Telephone	`ext<extension>@<IP address>`
IP Softphone	`ext<extension>@<IP address>`
Gateway Board	`gwp@<IP address>`
Gateway Box	`gwt@<IP address>`

SNMP Community ID

An authentication ID allowing read and/or write access to SNMP information. This is set as part of the VMM Server configuration. A single field is used to set both the SNMP Read Community ID and the SNMP Write Community ID.

A community ID with both read and write privileges must be available to VoIP Monitoring Manager (via the SNMP dialog box). When creating the community ID, ensure that it has both read AND write privileges.

SNMP Read Community ID

The read ID is necessary for obtaining information from the agent (for example, client queries and existing configuration settings). The read ID must match the ID defined in the Windows SNMP Service Properties dialog box.

SNMP Write Community ID

The write ID is necessary for sending information to the agent. The write ID must match the ID defined in the Windows SNMP Service Properties dialog box.

TTL Considerations

For a number of reasons, packets may not get delivered to their destination in a reasonable length of time. For example, a combination of incorrect routing tables could cause a packet to loop endlessly. A solution is to discard the packet after the packet has been forwarded a certain number of times and send a message to the originator, who decides whether to resend the packet.

The initial TTL value is set, usually by a system default, in a field of the IP packet header with a value in the range 0 to 255. The original idea of TTL was that it would specify a certain time span in seconds that, when exhausted, would cause the packet to be discarded.

Since each router is required to subtract at least one count from the TTL field, the count usually indicates the number of router hops the packet has remaining before it must be discarded. Each router that receives a packet subtracts one from the count in the TTL field. When the count reaches zero, the router detecting it discards the packet and sends an Internet Control Message Protocol (ICMP) message back to the originating host.

VoIP Monitoring Manager reports the TTL value detected by the endpoint for each RTP packet it receives.

Glossary

# #

802.1D: 802.1D is reported only if it is enabled.

802.1p: 802.1p is the IEEE endorsed Layer 2 traffic prioritization setting.

802.1Q: The 802.1Q field indicates the Virtual LAN to which this device has been assigned.

A

Acoustic Echo Cancellation: The acoustic echo cancellation metric indicates if an endpoint is configured for full-duplex, half-duplex or acoustic echo cancellation mode. The acoustic echo cancellation metric is an enumerated type metric. The possible values are: 0 = Half-duplex, 1 = Full-duplex, 2 = AEC. There is no acoustic echo cancellation on the VoIP engines. Acoustic echo cancellation is a feature for IP phones only.

Alarm: A Trap or Alarm is a message sent by a Windows SNMP Agent to a Trap Manager, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached. It is also referred to as an Alarm. The Trap Manager is typically configured to be the HP OpenView or Avaya Network Management Console but any Trap Manager application can be used with the AVAYA VoIP Monitoring Manager.

Apache: Apache HTTP server is an open-source HTTP server that is maintained by the Apache Software Foundation. A free download is available from http://www.apache.org. Follow the links to the HTTPD (HTTP daemon, web server). Note that Apache is installed as part of the Integrated Management Windows Server.

AVAYA-VMON-MIB: The AVAYA-VMON-MIB is used for the storage of VoIP Monitoring Manager trap configuration. (The ASN.1 definitions of this MIB and associated Traps are included as text files in the installation.)

C

Canonical Name: The canonical name or CNAME is the unique identifier for each participant within one RTP session, or set of related RTP sessions. The format is user@host, or host if a user name is not available as on single-user systems. For both formats, host is either the fully qualified domain name or IP address of the host from which the real-time data originates. For Avaya VoIP systems CNAMEs are of the format: IP Telephone: ext<extension>@<IP address>, IP Softphone: exs<extension>@<IP address>, Gateway Board: gwp@<IP address>, Gateway Box: gwt@<IP address>.

Child Endpoint: The terms parent and child endpoints are purely for describing the way endpoints are displayed in the Results List. A parent is like the branch in a tree view. A child is like a leaf in a tree view. The same endpoint can be shown as both a parent and a child. Click on the expanding icon positioned in the far left column of the Results List to expand the tree which displays a sub list with the child endpoints. A child endpoint represents a session between itself and its parent. This is different from a parent endpoint that just represents a physical endpoint.

CLAN: The CLAN is an IP interface (LAN interface) on an Avaya media server and provides control signalling to IP phones, Softphones, and other media gateways.

CNAME: Refer to Canonical Name.

Codec: A Codec is an encoder/decoder. In the context of RTP, it is the type of encoding used for the payload of the RTP packets exchanged as part of a conversation. For example, some RTP Codecs are G.723, G.711 aLaw and G.729. Session Properties shows which Codec is in use. RTP does not distinguish between different sub-types of codec (such as g729A and g729B).

D

Differentiated Services Code Point: The DiffServ Code Point (DSCP) metric represents the value of the IP DSCP field of the incoming RTP packets. The DSCP metric is a number in the range 0-63 and is used to specify the level of service a packet should receive whilst traversing the network.

DSCP: Refer to Differentiated Services Code Point.

E

Echo Tail Length: The echo tail length metric represents the length of echo cancellation processing determined by the distance between the gateway and the endpoint. The echo tail length metric is represented in milliseconds and can have typical value ranging from 8ms to 32ms.

Endpoint Type: The Results List displays an image representing the endpoint type in the left-hand column as follows: IP Phone - Standalone desk phone with a dedicated Ethernet dual hub, its own screen, handset, dial pad and feature access buttons; Soft Phone - Software only phone which is installed on any PC running the Windows operating system; Media Gateway - a network VoIP device.

EndTime: The EndTime column in the exported file displays the date and time the session ended. This column appears in the Session Table of the exported file.

F

Framesize: Frame size is the logical units into which data is partitioned for processing. In the case of a voice coder/decoder (codec) this is the time sliced blocks used by the codec algorithm. For example, the G.729 codec breaks the input audio signal into 10ms blocks for encoding purposes. Therefore, if the RTP packet payload is in 30ms blocks then there are 3 frames per packet. VoIP Monitoring Manager displays the framesize in the Session Properties tab of the report dialog.

G

Gatekeeper: The Gatekeeper column in the Session Table displays the media server or CLAN that controls the endpoint.

Gateway: A Gateway is generally used as a bridge between signaling protocols and bearer media. In this context, the Gateways allow IP endpoints to communicate with non-IP endpoints (e.g. the traditional circuit switched world of analogue and digital phones). AVAYA Gateways also perform the task of mixing the media channels in a conference call. A pair of Gateways can also be set up as an IP trunk.

H

HopAddress: The Hop Address column in the Trace Route Table is the IP address of each network node in the trace route.

HopCount: The HopCount column in the Trace Route Table indicates the hop number, that is, the position in the path node of the trace route.

HopTime: The HopTime column in the Trace Route Table displays in milliseconds the round-trip-time of the trace route packet, from the source to each path node in the trace route.

I

Interval: The period during which the specified number of warnings must be received to trigger an alarm (trap).

J

Jitter: Jitter is a measure of variance in the time it takes for communications to traverse from the sender (application) to the receiver, as seen from the application layer, or the difference between when a packet is supposed to be received and when it is actually received. Jitter is sometimes described as the statistical average variance in delivery time between packets or datagrams. Avaya VoIP Monitoring Manager reports Jitter in milliseconds.

Jitter Buffer Over Runs: The number of jitter buffer over-runs metric represents the number of times during a call the actual jitter exceeded the maximum size to which the jitter buffer is allowed to grow. This metric is an 8-bit unsigned integer.

Jitter Buffer Under Runs: The number of jitter buffer under-runs metric represents the number of times during a call the jitter buffer became empty or starved. This metric is an 8-bit unsigned integer.

L

Largest Sequence Fall: The Largest Sequence Fall metric represents the number of packets that are received later than expected, that is, after a higher-numbered packet was received. For example, if five packets arrive in the order 1, 2, 5, 3, 4, the largest sequence fall is 2 (generally indicating that 2 packets arrived later than expected). Note: A value of 0xFF implies that there were too many packets out of order to be able to calculate the correct value.

Largest Sequence Jump: The Largest Sequence Jump metric represents the maximum number of consecutive packets lost in the last RTCP reporting interval. It is based on sequence numbers assigned to packets as they are created. For example, when the following packet sequence numbers 1,2,3,8 are received, the largest Sequence Jump is 4. Note: A value of 0xFF implies that there were too many packets lost to be able to calculate the correct value.

LargestSeqFall: Refer to Largest Sequence Fall.

LargestSeqJump: Refer to Largest Sequence Jump.

M

Maximum Jitter: The Maximum Jitter metric represents the maximum value of jitter seen in the RTCP reporting interval. This metric would be useful to identify transient spikes of jitter in a session. This metric is a 32-bit unsigned integer. The unit is defined by the profile of the RTP session.

Media Encryption: The Media Encryption metric indicates whether media encryption is enabled or disabled for the RTP session. The Media encryption metric is an enumerated type metric. The possible values are: 0 = No encryption, 1 = AEA1.2, 2 = AES, 3-255 = Reserved for future use.

N

Number Sequence Falls: The number of sequence fall metric represents how many times during the RTP session there was at least one packet that was out of order.

Number Sequence Jumps: The number of sequence jump instances metric represents how many times during the reporting interval there was at least one packet which was lost.

NumberSeqFalls: Refer to Number Sequence Falls.

NumberSeqJumps: Number Sequence Jumps.

O

Octet: The Octet column in the Session Table indicates the size of the packets in octets.

P

Packet: A packet is the logical grouping of information that includes a header containing control information and (usually) the user data. The term packet is most often used to refer to the application layer data units.

Parent Endpoint: The terms parent and child endpoints are purely for describing the way endpoints are displayed in the Results List. A parent is like the branch in a tree view. A child is like a leaf in a tree view. The same endpoint can be shown as both a parent and a child. A parent endpoint is any endpoint listed as a result of a search. You click on the expanding key icon positioned in the far left column to expand the parent endpoint and show the child endpoints.

ParticipantID: The ParticipantID column assigns a unique identifier to each participant in the exported file. Each exported session has two participants. The exported data contains three sets of data. This data is listed in three separate tables that are separated by a blank row: Session Table, Time-varying Data Table and the TraceRoute Table. For every session a participant was involved in there will be a unique pair: SessionID and ParticipantID, enabling you to associate the session data, time-varying data and the trace route data as belonging to that participant in a specific session. Use the ParticipantID to identify the participant in each table to analyze the data.

Payload: Payload refers to the contents of a packet. In RTP it is encoded audio that is the user data of a packet. The payload identifies which codec is being used.

Perceived Delay: Perceived delay is the total effect RTT and Jitter have on a phone user's conversation.

Q

QoS: Refer to Quality of Service.

Quality of Service: QoS is the measure of the level of quality that a service requires or receives. The VoIP Monitoring Manager monitors and displays the 3 main factors that determine the quality of VoIP calls. These factors are Jitter, Round Trip Time, and Packet Loss. On the Summary Report each of the three factors display as a separate gauge.

R

RcvrIPAddr: The RcvrIPAddr column displays the IP address of this session participant (i.e. endpoint). This column appears in the Session Table of the exported file.

RcvrPHONE: The RcvrIPAddr column displays the phone number of the participant. This column appears in the Session Table of the exported file.

Real-Time Transport Control Protocol: A protocol providing support for applications with real-time properties, including timing reconstruction, loss detection, security, and content identification. It reports information about the RTP stream.

Real-Time Transport Protocol: Real-Time Transport Protocol is the protocol used for transmitting real-time data. For more information see IETF RFC 1889 located at: http://www.ietf.org/rfc/rfc1889.txt

Resource ReSerVation Protocol: RSVP is a protocol for reserving network bandwidth on the routers and switches between two endpoints in a session (in some other protocol, such as RTP). There are two reservations per session, one for each direction the data has to travel. For further reference see the IETF RFCs 2205 and 2750 located at: http://www.ietf.org/rfc/rfc2205.txt and http://www.ietf.org/rfc/rfc2750.txt

Round Trip Time: Round trip time is the length of time (in milliseconds) it takes a packet to traverse the network and return (thus being a round trip). It is the sum of the two one-way network delays between two endpoints. Callers can experience difficulties in carrying on a normal conversation when the one-way network delay exceeds 500 milliseconds (ms). However, some users may elect to tolerate this.

RSVP: Refer to Resource ReSerVation Protocol.

RSVP Status: The RSVP status for an endpoint shows whether the RSVP is enabled on the endpoint, and if it is, whether a reservation was established for the received RTP data stream.

RTCP: Refer to Real-Time Transport Control Protocol.

RTCP Listen Port: The RTCP Listen Port is the configurable port that is used to collect RTCP information from the AVAYA endpoints. The number must be from 1025 through 65535. The default port is 5005. Users are advised to avoid choosing ports in the reserved and 'well-known' ranges.

RTP: Refer to Real-Time Transport Protocol.

RTP MIB: The RTP MIB stores the information for the active RTP Sessions. The reference for the definition of the RTP MIB is located at: http://www.ietf.org/rfc/rfc2959.txt

RTP Session: A session is a VoIP connection between two IP endpoints. For more information see RFC 1889 located at: http://www.ietf.org/rfc/rfc1889.txt

RTT: Refer to Round Trip Time.

S

Session Table: The Session table is the exported table containing data that generally remains the same during a session. As a result, there is one entry per session in this table. The Session table will display in Microsoft Excel at the top of the same worksheet as the Time-varying Data table and the Trace Route table. The data in the Session table is indexed by SessionID and ParticipantID.

SessionID: The SessionID column assigns a unique identifier to each session in the exported file. Each exported session contains three sets of data. This data is listed in three separate tables that are separated by a blank row: Session Table, TimeStamped DataTable and the TraceRoute Table. Use the SessionID to identify the session in each table to analyze the data.

Silence Suppression: In Voice over IP (VoIP), silence suppression is a method of detecting the silence in audio and purposefully dropping silent packets at the sender to conserve network bandwidth. The receiver will generate comfort noise or conceal the loss of packets when packets are dropped. Because the receiver conceals loss and generates comfort noise, silence suppression is usually imperceptible to the listener. The silence suppression will be reported as enabled, disabled or unknown.

Simple Network Management Protocol: SNMP is a standard protocol for communicating with network devices.

SNMP: Refer to Simple Network Management Protocol.

StartTime: The StartTime column in the exported file displays the date and time the session started. This column appears in the Session Table of the exported file.

T

Time-To-Live: Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router if a packet has been forwarded towards its destination too many times and should be discarded.

Time-varying Data Table: The Time-varying Data table is one of the exported tables containing the time-varying data for the sessions in the Session table. The data in this table is indexed by SessionID, ParticipantID, and a time offset. The SessionID and ParticipantID enable the data to be linked to corresponding sessions in the Session table. The time offset indicates when this set of information was reported (in seconds since the start of each call). The Time-varying Data table will display in Microsoft Excel below the Session table on the same worksheet. To view the information more easily, you may want to copy the table and paste it to another worksheet.

TimeOffset: The TimeOffset column displays the number of seconds since the session started for this set of data. This column appears in the Time-varying Data Table of the exported file.

TOOL: The TOOL value is the name and version of the application generating the stream, for example, Avaya VoIP Engine v.123. This information may be useful for diagnosis. The TOOL value should remain constant for the duration of the session.

Trace Route Table: The Trace Route table contains information about the route in the network that the RTP packets traverse between the two endpoints of the call. It will display in Microsoft Excel below the Time-varying Data table.

Trap: Refer to Alarm

TTL: Refer to Time-To-Live.

V

Voice over Internet Protocol: Voice over Internet Protocol (VoIP) is the technology standard that supports Internet telephony. It provides the capability for live voice communication over the Internet so that you can talk using the multimedia capabilities of your computer, in the same way you would talk using a telephone.

VoIP: Refer to Voice over Internet Protocol.

W

Windows SNMP Agent: The Windows SNMP Agent runs as an operating-system-managed service. It is optionally installed with the Windows Operating System.

Index

1

10MB 57

162....72

A

About AVAYA VoIP Mon 68

About AVAYA VoIP Monitoring Manager

- Components of VoIP Monitoring Manager 2
- VoIP Monitoring Manager Client....13
- VoIP Monitoring Manager Server.....61, 72

About AVAYA VoIP Monitoring Manager 1

About Detailed Reports 32

About RTCP Monitor 56

About Session Properties....34

About Summary Reports 31

About the Database....57

About VoIP Monitoring Manager 1

About VoIP Monitoring Manager Client....2

About VoIP Monitoring Manager Server....2

About VoIP Monitoring Manager Web Client 2

Access Error 67

Active Endpoints

- Results List....17
- Search Dialog....16, 24

Active Endpoints....28

Activity Monitor 57

Advanced Search

- Invalid Search Parameter 68
- Run a Search 21, 23
- Search Dialog....16, 24
- Search for a Specific Network Address .25
- Search for a Specific Phone Number 26
- Search Using Quality of Service (QoS) Values....27

Advanced Search 24

Alarms

- Call Alarms 64
- Generating Traps & Alarms.... 63
- System Alarms 65
- Terminal Alarms 66

aliases.... 28

Alter

- Altering Date Range of Reports 46
- Arrange the Reports on the Screen 49
- Connect to a New Server 23
- Copy to Clipboard.... 44
- Host Name Server dialog 11
- Search Dialog.... 16, 24

Alter.... 46

Altering Date Range of Reports.... 46

Applet

- Components of VoIP Monitoring Manager 2
- Connect to New Server 23
- Copy 44

Applet.... 20

Applet.... 60

Arrange Icons.... 49

Arrange the Reports on the Screen

- Cascade Reports.... 50
- Close All Reports.... 44
- Close Report 44
- Maximize Reports.... 49
- Minimize the Reports 50
- Move the Reports 44
- Tile Horizontally.... 50
- Tile Vertically.... 49
- View Multiple Reports 50

Arrange the Reports on the Screen.... 49

AVAYA-VMON-MIB

- Components of VoIP Monitoring Manager 2

B

Binding 72

Blank Fields 70

Browser

- About VoIP Monitoring Manager Web Client 2
- Connect to New Server 23
- Copy 44
- Web Client Time Displays an Incorrect Time 71

Browser 2

C

Call Alarms

- Configure SNMP Service For Sending Traps 9
- Generating Traps & Alarms 63
- RTCP or Real-Time Transport Control Protocol 75
- System Alarms 65
- Terminal Alarms 66

Call Alarms 64

Canonical Name CNAME 82

Cascade Reports

- Arrange the Reports on the Screen 49
- View Multiple Reports 50

Cascade Reports 50

Check for a Valid Community ID

- VoIP Monitoring Manager Server Properties 53
- Windows SNMP Agent 71

Check for a Valid Community ID 8

Check Windows SNMP Agent is Installed and Running 7

Child Endpoint

- Difference Between Endpoint and Session Reports 35
- How Sessions Display in a Report 50
- Results List 17

Client

- Components of VoIP Monitoring Manager 2
- How to Start VoIP Monitoring Manager 20, 60
- How to Use VoIP Monitoring Manager Client 20
- VoIP Monitoring Manager Server ... 61, 68, 72

Client 13

Close All Reports 44

Close Report 44

Community ID

- Check for a Valid Community ID 8
- VoIP Monitoring Manager Server Properties 53
- Windows SNMP Agent 71
- Windows SNMP Agent Connection Error 71

Community ID 8

Components of VoIP Monitoring Manager

- About RTCP Monitor 56
- About Summary Reports 31
- About VoIP Monitoring Manager 1
- About VoIP Monitoring Manager Client ... 2
- About VoIP Monitoring Manager Server . 2
- About VoIP Monitoring Manager Web Client 2
- RTCP or Real-Time Transport Control Protocol 75
- Starting VoIP Monitoring Manager Web Client 20, 60
- VoIP Monitoring Manager Server Properties 53
- Windows SNMP Agent 71

Components of VoIP Monitoring Manager . 2

Configure AVAYA Switch Administration Forms

- Configure IP-Network-Region form 6
- Generating Traps & Alarms 63

Configure Database 11

Configure IP-Network-Region form
Generating Traps & Alarms 63
Configure IP-Network-Region form 6
Configure SNMP Service For Sending Traps
Generating Traps & Alarms 63
Configure SNMP Service For Sending Traps 9
Configure System-Parameters IP-Options Form 7
Connect to Database 10
Connect to New Server
Host Name Server dialog 11
Starting VoIP Monitoring Manager Web Client 20, 60
Connect to New Server 23
Connect to RTCP Monitor 62
Connection
Could Not Resolve Host Name 71
Error Messages 67
How to Start VoIP Monitoring Manager 20, 60
SNMP Service Error 74
Starting VoIP Monitoring Manager Web Client 20, 60
Troubleshooting 67
Windows SNMP Agent Connection Error 71
Connection 16
Connection 23
Connection Status
Status Bar 16
Connection Status 16
Copy
Starting VoIP Monitoring Manager Web Client 20, 60
Copy 44
Could Not Communicate with the Windows SNMP Agent
Windows SNMP Agent 71
Windows SNMP Agent Connection Error 71
Could Not Communicate with the Windows SNMP Agent 74
Could Not Resolve Host Name
Troubleshooting 67
VoIP Monitoring Manager Server ... 61, 68, 72
Could Not Resolve Host Name 71
Creating Reports with Exported Data . 28, 52

D

Data
How Sessions Display in a Report 50
Jitter 81
Migration 11
No Data is Displaying on a Report 68
No Endpoint Data Available 68
No Endpoints Matched the Given Search 69
Round Trip Time (RTT) 57
Summary Data Stored 57
View a Report 22, 43
Data 11
Data Storage 57
Data Stored 57
Database 57
Database Schema 75
Date Range 46
Date Range is Invalid
Error Messages 67
Run a Search 21, 23
Date Range is Invalid 68
Detailed Media Gateway Link report 41
Detailed Report
Interpreting the Values Using Detailed Reports 47
Update All Reports Now 45
X-axis 48
Y-axis 48

Detailed Report....32
Detailed Session Report
About Detailed Reports....32
How Sessions Display in a Report....50
Summary Session Report....35
Update All Reports Now....45
Detailed Session Report....38
Diagram
Entity Relationship....80
Diagram....80
Dialog
About Detailed Reports....32
About Summary Reports....31
Advanced Search....24
Overview of VoIP Monitoring Manager..20
Search Dialog....16, 24
VoIP Monitoring Manager Server....61, 68, 72
Dialog....53
Difference Between Endpoint and Session Reports
How Sessions Display in a Report....50
Difference Between Endpoint and Session Reports....35
Display
Altering Date Range of Reports....46
Arrange the Reports on the Screen....49
Connection Status....16
Host Name Server dialog....11
How Sessions Display in a Report....50
Jitter....81
List All Active Endpoints....28
Minimize the Reports....50
No Data is Displaying on a Report....68
Round Trip Time (RTT)....57
Search Dialog....16, 24
Tile Horizontally....50
Tile Vertically....49
View a Report....22, 43
View Multiple Reports....50
View Results List....27
View Status Bar....28
View ToolBar....19
VoIP Monitoring Manager Server Properties....53
Display....13
Display....20
Display....60
Display....61
Display....72

E

Edit
Advanced Search....24
Altering Date Range of Reports....46
Arrange the Reports on the Screen....49
Configure IP-Network-Region form....6
Configure SNMP Service For Sending Traps....9
Connect to New Server....23
Edit Report Properties....45
Generating Traps & Alarms....63
Edit....46
Edit Menu - Client
Edit Report Properties....45
Search Button....19
Update All Reports....45
Edit Menu - Client....45
Edit Report Properties....45
Endpoint
About Detailed Reports....32
About Summary Reports....31
Gateway....48
How Sessions Display in a Report....50
Interpreting the Values Using Detailed Reports....47

Interpreting the Values Using Summary Reports 47
List All Active Endpoints 28
No Endpoints Matched the Given Search 69
Results List 17
Search Dialog 16, 24
Search for a Specific IP Address 25
Search for a Specific Phone Number 26
Search Using Quality of Service (QoS) Values 27
Endpoint 35
Endpoint Type
Gateway 48
Results List 17
endpoints 14
Enter a Percentage Loss Less than 100 68
Entity Relationship Diagram 80
Error Message
Access Error 67
Could Not Communicate with the SNMP Agent 74
Could Not Resolve Host Name 71
General Server Error 72
Help Could Not Be Displayed 67
Invalid Bounds - Loss Report Properties Dialog 68
Invalid Date Range 68
Invalid RTCP Port 72
No Data is Displaying on a Report 68
No Endpoint Data Available 68
No Endpoints Matched the Search 69
Report Limit Reached 67
RMI Registry Error 73
Server Unavailable 69
Server Version Error 70
Set RTCP Port Error 73
SNMP Service Error 74
Troubleshooting 67
Unknown Error 70
VoIP Monitoring Manager Server Error Messages 71
Windows SNMP Agent Connection Error 71
Windows SNMP Agent is Not Running 74
Error Message 67
Error Message 71
Error Messages 67
Excel 27, 51, 52
Export Report Data
Create Statistical Reports 28, 52
Some Fields Are Blank in the Exported Data 70
Export Report Data 52
Export Result List
Create Statistical Reports 28, 52
Some Fields Are Blank in the Exported Data 70
Export Result List 27
Export Result List 51

F

File Menu - Client
Connect to New Server 23
File Menu - Client 23
firewall 72

G

Gateway 48
gateways 28
General Server Error 72
Generating Traps & Alarms 63
Getting Started
How to Start VoIP Monitoring Manager 20, 60
How to Use VoIP Monitoring Manager Client 20
Installing VoIP Monitoring Manager Server 5
Run a Search 21, 23

Starting VoIP Monitoring Manager Web Client 20, 60
View a Report..... 22, 43
VoIP Monitoring Manager Client 13
Getting Started..... 5
Getting Started..... 20
Getting Started..... 20
Getting Started..... 60
Glossary
Jitter 81
Real-Time Transport Control Protocol (RTCP) 75
Round Trip Time (RTT)..... 57
RSVP Status 81
Troubleshooting 67
Windows SNMP Agent..... 74
Graph Limit Reached..... 67

H

Help Could Not Be Displayed..... 67
Help Icon..... 4
Host Name
Connect to a New Server..... 23
Could Not Resolve Host Name..... 71
Host Name Server dialog..... 11
Search Dialog..... 16, 24
Troubleshooting 67
Host Name..... 11
Host Name Server dialog 11
How Sessions Display in a Report
About Detailed Reports..... 32
About Summary Reports..... 31
Detailed Session Report 38
Difference Between Endpoint and Session Reports..... 35
Summary Session Report..... 35
How Sessions Display in a Report 50
How to Check for a Valid Community ID
VoIP Monitoring Manager Server Properties 53
Windows SNMP Agent..... 71
How to Check for a Valid Community ID 8
How to Start VoIP Monitoring Manager ... 20, 60
How to Use VoIP Monitoring Manager Client
Run a Search 21, 23
View a Report..... 22, 43
VoIP Monitoring Manager Client 13
How to Use VoIP Monitoring Manager Client 20
How to...
Altering Date Range of Reports 46
Arrange the Reports on the Screen 49
Check for a Valid Community ID 8
Configure SNMP Service For Sending Traps..... 9
Connect to a New Server 23
Generating Traps & Alarms..... 63
How to Start VoIP Monitoring Manager 20, 60
How to Use VoIP Monitoring Manager Client..... 20
Installing VoIP Monitoring Manager Server 5
Interpreting the Values Using Detailed Reports 47
Interpreting the Values Using Summary Reports 47
Run a Search 21, 23
Search for a Specific Network Address 25
Search for a Specific Phone Number.... 26
Search Using Quality of Service (QoS) Values..... 27
Starting VoIP Monitoring Manager Web Client..... 20, 60
View a Report..... 22, 43
View Multiple Reports 50
How to... 5
How to... 20

How to....20
How to....60
I
Information
Error Messages....67
Information....4
Installing VoIP Monitoring Manager Server
Check for a Valid Community ID....8
Check Windows SNMP Agent is Installed and Running....7
How to Start VoIP Monitoring Manager 20, 60
Starting VoIP Monitoring Manager Web Client....20, 60
VoIP Monitoring Manager Server....61, 68, 72
Windows SNMP Agent....71
Installing VoIP Monitoring Manager Server.5
Internet Explorer....20, 60
Interpreting the Values Using Detailed Reports
About Detailed Reports....32
Interpreting the Values Using Detailed Reports....47
Interpreting the Values Using Summary Reports
About Summary Reports....31
Interpreting the Values Using Summary Reports....47
Invalid Bounds....68
Invalid Date Range
Error Messages....67
Search Dialog....16, 24
Invalid Date Range....68
Invalid RTCP Port
Error Messages....67
Invalid RTCP Port....72
Invalid Search Parameter
Advanced Search....24
Invalid Search Parameter....68
IP Address
Results List.... 17
Search Dialog.... 16, 24
Search for a Specific IP Address 25
IP Address 25
IP addresses 28
ip-network-region form 6
J
Java Policy File 67
Jitter
Round Trip Time (RTT) 57
Jitter 81
L
license server 62
licenses 3, 30, 59, 62, 67
Limit 57
M
Maximize Reports 49
Media Gateway Link report 39, 41, 43
MIB
Components of VoIP Monitoring Manager 2
Migrate Data 11
Minimize the Reports
Arrange the Reports on the Screen 49
Minimize the Reports 50
Monitor
Components of VoIP Monitoring Manager 2
Connect to a New Server 23
Monitor 2
Move the Reports
Arrange the Reports on the Screen 49
Copy 44
Move the Reports.... 44

N

Network Address
- Invalid Search Parameter 68
- Results List 17
- Search Dialog 16, 24

Network Address 25

New Search
- Results List 17
- Search Dialog 16, 24
- Search for a Specific Network Address 25
- Search for a Specific Phone Number 26
- Search Using Quality of Service (QoS) Values 27

New Search 19

No Data is Displaying on a Report
- Error Messages 67

No Data is Displaying on a Report 68

No Endpoint Data Available
- Error Messages 67

No Endpoint Data Available 68

No Endpoints Matched the Search
- Configure IP-Network-Region form 6
- Run a Search 21, 23
- Search Dialog 16, 24

No Endpoints Matched the Search 69

O

Options 53

Organize
- Arrange the Reports on the Screen 49
- Cascade Reports 50
- Close All Reports 44
- Close Report 44
- Maximize Reports 49
- Minimize the Reports 50
- Move the Reports 44
- Tile Horizontally Reports 50
- Tile Vertically Reports 49
- View Results List 27
- View Status Bar 28
- View ToolBar 19

Organize 49

Overview of VoIP Monitoring Manager Client
- Components of VoIP Monitoring Manager 2
- Connection Status 16
- Error Messages 67
- Status Bar 16
- Troubleshooting 67
- VoIP Monitoring Manager Client 13
- VoIP Monitoring Manager Server ... 61, 68, 72

Overview of VoIP Monitoring Manager Client 20

P

Packet Loss
- Jitter 81
- Round Trip Time (RTT) 57

Parent Endpoint
- Difference Between Endpoint and Session Reports 35
- How Sessions Display in a Report 50
- Results List 17

Perceived Delay
- Jitter 81
- Round Trip Time (RTT) 57

Phone Number
- Search Dialog 16, 24
- Search for a Specific Phone Number 26

Phone Number 26

Port
- Components of VoIP Monitoring Manager 2
- Invalid RTCP Port 72
- Problems with Binding to Port 162 72
- Set RTCP Port Error 73
- SNMP Agent 71

VoIP Monitoring Manager Server....61, 68, 72
Port 72
Ports used by Server 72
Problems Binding to Port 162....72
Programs
Components of VoIP Monitoring Manager 2
Starting VoIP Monitoring Manager Web Client 20, 60
VoIP Monitoring Manager Client....13
VoIP Monitoring Manager Server....61
Windows SNMP Agent....71
Programs 20
Programs 60
Properties
Edit Report Properties....45
VoIP Monitoring Manager Options....53
Properties 53

Q

Quality of Service (QoS)
Jitter 81
Round Trip Time (RTT)....57
Search Using Quality of Service (QoS) Values....27

R

Real-Time Transport Control Protocol (RTCP) 75
Recommended Alarm Settings....63
Relationship Diagram 80
Report
About Detailed Reports....32
About Summary Reports....31
Altering Date Range of Reports....46
Arrange the Reports on the Screen 49
Detailed Session Report 38
Difference Between Endpoint and Session Reports 35
Edit Report Properties....45
How Sessions Display in a Report 50
Interpreting the Values Using Detailed Reports 47
Interpreting the Values Using Summary Reports 47
Maximize Reports....49
Minimize the Reports 50
Move the Reports....44
Summary Session Report 35
Update All Reports 45
Update Report....45
View a Report....22, 43
View Multiple Reports 50
Report 32
Report Data
Results List....17
Search Dialog....16, 24
Summary Data Stored....57
Report Data....17
Report Limit Reached 67
Report Properties Dialog
About Detailed Reports 32
About Summary Reports....31
Edit Report Properties....45
Invalid Bounds....68
Report Properties Dialog 45
Reports
About Detailed Reports 32
About Summary Reports....31
Altering Date Range of Reports 46
Arrange the Reports on the Screen 49
Detailed Session Report 38
Difference Between Endpoint and Session Reports 35
How Sessions Display in a Report 50
Interpreting the Values on a Summary Report 47
Interpreting the Values Using Detailed Reports 47

Maximize Reports 49
Minimize the Reports 50
Move the Reports....44
Summary Session Report....35
Update All Reports....45
Update Report....45
View a Report....22, 43
View Multiple Reports 50
Reports 31
Reports 32
Results List
Gateway....48
Search Button 19
View a Report....22, 43
View Active Endpoints 28
View Results List....27
VoIP Monitoring Manager Client....13
Results List 17
RMI Registry Error
Troubleshooting 67
RMI Registry Error....73
Round Trip Time (RTT)
Jitter 81
Round Trip Time (RTT) 57
RSVP Status....81
RTCP Listen Port....62
RTCP Monitor
Components of VoIP Monitoring Manager 2
Installing VoIP Monitoring Manager Server 5
RTCP Monitor....56
RTCP or Real-Time Control Protocol 75
RTCP or Real-Time Transport Control Protocol....75
RTP Stream Table
Create Statistical Reports 28, 52
Export Report Data 52
Export Result List 27, 51
Run a Search 21, 23

S

SAT
Configure IP-Network-Region Form.... 6
SAT 53
Scales 48
Schema - database.... 75
Search
Advanced Search.... 24
Altering Date Range of Reports 46
Gateway 48
Invalid Search Parameter.... 68
No Endpoints Matched the Search 69
Results List.... 17
RSVP Status 81
Run a Search 21, 23
Search Button.... 19
Search Dialog.... 16, 24
Search for a Specific Network Address 25
Search for a Specific Phone Number.... 26
Search Using Quality of Service (QoS) Values.... 27
Search.... 16
Search.... 21
Search.... 23
Search.... 24
Search Button 19
Search Dialog
Advanced Search.... 24
Invalid Date Range.... 68
Invalid Search Parameter.... 68
Results List.... 17
Run a Search 21, 23
Search Dialog 16
Search Dialog 24

Search for a Specific IP Address
Advanced Search....24
Search for a Specific IP Address....25
Search for a Specific Network Address
Advanced Search....24
Search for a Specific Network Address....25
Search for a Specific Phone Number
Advanced Search....24
Search for a Specific Phone Number....26
Search Using Quality of Service QoS Values
Advanced Search....24
Search Using Quality of Service QoS Values....27
Server
About VoIP Monitoring Manager Server..2
Check for a Valid Community ID....8
Components of VoIP Monitoring Manager....2
Connect to New Server....23
General Server Error....72
Host Name Server dialog....11
Installing VoIP Monitoring Manager Server....5
Invalid RTCP Port....72
RMI Registry Error....73
Server Unavailable....69
Server Version Error....70
Starting VoIP Monitoring Manager Web Client....20, 60
VoIP Monitoring Manager Server....61, 68, 72
VoIP Monitoring Manager Server Error Messages....71
VoIP Monitoring Manager Server Properties....53
Server....2
Server....61
Server....68
Server....72
Server Already Running
Error Messages....67
Server cannot Connect to SNMP....73
Server Could Not Reconnect to the SNMP Agent
Error Messages....67
Windows SNMP Agent....71
Server Could Not Reconnect to the SNMP Agent....71
Server Error Messages....71
Server Properties....53
Server Unavailable
Error Messages....67
How to Start VoIP Monitoring Manager 20, 60
VoIP Monitoring Manager Server... 61, 68, 72
Server Unavailable....69
Server Version Error
Change Server....23
Error Messages....67
Host Name Server dialog....11
VoIP Monitoring Manager Server... 61, 68, 72
Server Version Error....70
Session
Difference Between Endpoint and Session Reports....35
How Sessions Display in a Report....50
Results List....17
Session....35
Set RTCP Port Error
Windows SNMP Agent....71
Set RTCP Port Error....73
Size....57
SNMP Agent
Check for a Valid Community ID....8
Components of VoIP Monitoring Manager....2

Configure SNMP Service For Sending Traps 9
Could Not Communicate with the Windows SNMP Agent 74
Set RTCP Port Error 73
SNMP Service Error 74
VoIP Monitoring Manager Server Properties 53
Windows SNMP Agent 71
Windows SNMP Agent Connection Error 71
Windows SNMP Agent is Not Running .. 74
SNMP Agent 71
SNMP Connection Error
Check for a Valid Community ID 8
Error Messages 67
Windows SNMP Agent 71
Windows SNMP Agent is Not Running .. 74
SNMP Connection Error 71
SNMP Service Error
Windows SNMP Agent 71
Windows SNMP Agent is Not Running .. 74
SNMP Service Error 74
Some Fields Are Blank in the Exported Data 70
Starting VoIP Monitoring Manager
Components of VoIP Monitoring Manager 2
How to Use VoIP Monitoring Manager Client 20
Installing VoIP Monitoring Manager Server 5
Starting VoIP Monitoring Manager Web Client 20, 60
Windows SNMP Agent 71
Starting VoIP Monitoring Manager 20
Starting VoIP Monitoring Manager 60
Starting VoIP Monitoring Manager Web Client
Connect to New Server 23
Copy 44
How to Use VoIP Monitoring Manager Client 20
VoIP Monitoring Manager Server ... 61, 68, 72
Starting VoIP Monitoring Manager Web Client 20
Starting VoIP Monitoring Manager Web Client 60
Status Bar
Connection Status 16
View Status Bar 28
Status Bar 16
Storage 57
Summary Media Gateway Link report 39
Summary Report
Interpreting the Values Using Summary Reports 47
Summary Report 31
Summary Session Report
About Summary Reports 31
Difference Between Endpoint and Session Reports 35
How Sessions Display in a Report 50
Interpreting the Values Using Summary Reports 47
Summary Session Report 35
SUN 20, 60, 67
Support Details 4
Switch Administration Forms
Configure IP-Network-Region form 6
System Alarms
Call Alarms 64
Configure SNMP Service For Sending Traps 9
Generating Traps & Alarms 63
Terminal Alarms 66
System Alarms 65
System pane 13
System Requirement - Port 1099 7

System View 28
system-parameters ip-options form
Configure IP-Network-Region form 6
T
Terminal Alarms
Call Alarms 64
Configure SNMP Service For Sending Traps 9
Generating Traps & Alarms 63
System Alarms 65
Terminal Alarms 66
Tile Horizontally 50
Tile Vertically 49
Time Stamp Table
Create Statistical Reports 28, 52
Export Report Data 52
Export Result List 27, 51
Time-To-Live TTL 83
Tool Bar
Connect to a New Server 23
Copy 44
Edit Report Properties 45
Export Result List 27, 51
Help 4
New Search 19
View Active Endpoints 28
View Results List 27
View Status Bar 28
View ToolBar 19
Tool Bar 23
Trace Route Table
Create Statistical Reports 28, 52
Export Report Data 52
Export Result List 27, 51
Trace Routes Media Gateway Link report . 43
Trap or Alarm
Call Alarms 64
Configure SNMP Service For Sending Traps 9
Generating Traps & Alarms 63
Recommended Settings 63
System Alarms 65
Terminal Alarms 66
Trap or Alarm 63
Troubleshooting Problems with Client
Check for a Valid Community ID 8
No Data is Displaying on a Report 68
No Endpoint Data Available 68
No Endpoints Matched the Search 69
Windows SNMP Agent is Not Running . 74
Troubleshooting Problems with Client 67
Troubleshooting Problems with Server
Check for a Valid Community ID 8
Could Not Resolve Host Name 71
Invalid RTCP Port 72
Proble 72
RMI Registry Error 73
Set RTCP Port Error 73
SNMP Service Error 74
VoIP Monitoring Manager Server Error Messages 71
Windows SNMP Agent Connection Error 71
U
Unable to establish database connection . 74
Understanding Detailed Reports
About Detailed Reports 32
Detailed Session Report 38
Interpreting the Values Using Detailed Reports 47
Understanding Detailed Reports 32
Understanding Summary Reports
About Summary Reports 31
Interpreting the Values Using Summary Reports 47
Summary Session Report 35

Understanding Summary Reports 31
Unknow Endpoint - in report 68
Unknown Error
Error Messages 67
Unknown Error 70
Update All Reports 45
Update Report 45
Using Client
How to Start VoIP Monitoring Manager 20, 60
Installing VoIP Monitoring Manager Server 5
VoIP Monitoring Manager Client 13
VoIP Monitoring Manager Server 61, 68, 72
Using Client 20
Using Server
How to Start VoIP Monitoring Manager 20, 60
Installing VoIP Monitoring Manager Server 5
Starting VoIP Monitoring Manager Web Client 20, 60
VoIP Monitoring Manager Client 13
VoIP Monitoring Manager Server Error Messages 71
VoIP Monitoring Manager Server Properties 53
Using Server 61
Using Server 68
Using Server 72
V
View
Active Endpoints 28
Detailed Session Report 38
Host Name Server dialog 11
How Sessions Display in a Report 50
Maximize Reports 49
No Data is Displaying on a Report 68
Results List 17
Search Dialog 16, 24
Starting VoIP Monitoring Manager Applet 20, 60
Summary Session Report 35
View a Report 22, 43
View Multiple Reports 50
View Results List 27
View Status Bar 28
View ToolBar 19
VoIP Monitoring Manager Server ... 61, 68, 72
VoIP Monitoring Manager Server Properties 53
View 28
View a Report
About Detailed Reports 32
About Summary Reports 31
Arrange the Reports on the Screen 49
Detailed Session Report 38
How Sessions Display in a Report 50
Interpreting the Values Using Detailed Reports 47
Interpreting the Values Using Summary Reports 47
Results List 17
Summary Session Report 35
View Multiple Reports 50
View a Report 22
View a Report 43
View Active Endpoints 28
View Menu
View Results List 27
View Status Bar 28
View ToolBar 19
View Menu 27
View Multiple Reports
Arrange the Reports on the Screen 49
View Multiple Reports 50
View Results List

Results List....17
Search Dialog....16, 24
VoIP Monitoring Manager Client....13
View Results List....27
View Sessions
Difference Between Endpoint and Session Reports....35
How Sessions Display in a Report....50
View Sessions....50
View Sessions in a Report....50
View Status Bar
Connection Status....16
Status Bar....16
View Status Bar....28
View ToolBar....19
VoIP Monitoring Manager Client
About VoIP Monitoring Manager Client....2
Components of VoIP Monitoring Manager....2
How to Start VoIP Monitoring Manager 20, 60
How to Use VoIP Monitoring Manager Client....20
Installing VoIP Monitoring Manager Server....5
Starting VoIP Monitoring Manager Web Client....20, 60
VoIP Monitoring Manager Server....61, 68, 72
VoIP Monitoring Manager Client....13
VoIP Monitoring Manager Client....20
VoIP Monitoring Manager Client....60
VoIP Monitoring Manager Options....53
VoIP Monitoring Manager Server
About VoIP Monitoring Manager Server....2
Components of VoIP Monitoring Manager....2
How to Start VoIP Monitoring Manager 20, 60
Installing VoIP Monitoring Manager Server....5
Invalid RTCP Port....72
Starting VoIP Monitoring Manager Web Client....20, 60
VoIP Monitoring Manager Server Error Messages....71
VoIP Monitoring Manager Server Properties....53
VoIP Monitoring Manager Server....61
VoIP Monitoring Manager Server....68
VoIP Monitoring Manager Server....72
VoIP Monitoring Manager Server Error Messages....71
VoIP Monitoring Manager Server Properties....53

W

Warning....64, 65
Web Client
Components of VoIP Monitoring Manager....2
Connect to New Server....23
Copy....44
Starting VoIP....20, 60
Web Client Time Displays an Incorrect Time....71
Web Client....2
Web Client Time Displaying Incorrect Time....71
Web Client Time Displays an Incorrect Time....71
WebLM....62
What is this...
About Detailed Reports....32
About Summary Reports....31
Access Error....67
Detailed Session Report....38
Gateway....48
General Server Error....72
Host Name Server dialog....11

Jitter 81
Real-Time Transport Control Protocol (RTCP) 75
Results List....17
RMI Registry Error 73
Round Trip Time (RTT)....57
RSVP Status 81
Server Version Error 70
SNMP Service Error....74
Summary Session Report 35
VoIP Monitoring Manager Client....13
VoIP Monitoring Manager Server....61, 68, 72
Windows SNMP Agent....71
X-axis 48
Y-axis 48
What is this... 32
What is...
Gateway....48
General Server Error....72
Jitter 81
Real-Time Transport Control Protocol (RTCP) 75
RMI Registry Error 73
Round Trip Time (RTT)....57
RSVP Status 81
RTCP Monitor 2
SNMP Service Error....74
VoIP Monitoring Manager Client....13
VoIP Monitoring Manager Server....61
Windows SNMP Agent....71
Window Menu
Arrange Icons....49
Arrange the Reports on the Screen 49
Cascade Reports.... 50
Close All Reports.... 44
Close Report 44
Maximize Reports.... 49
Minimize the Reports 50
Tile Horizontally.... 50
Tile Vertically.... 49
Window Menu 49
Windows SNMP Agent
Check for a Valid Community ID 8
Check Windows SNMP Agent is Installed and Running 7
Components of VoIP Monitoring Manager 2
Configure SNMP Service For Sending Traps.... 9
Could Not Communicate with the SNMP Agent 74
Set RTCP Port Error.... 73
SNMP Service Error 74
VoIP Monitoring Manager Server... 61, 68, 72
Windows SNMP Agent is Not Running . 74
Windows SNMP Agent 71
Windows SNMP Agent Connection Error . 71
Windows SNMP Agent is Not Running..... 74
X
X-axis
About Detailed Reports 32
X-axis 48
Y
Y-axis
About Detailed Reports 32
Y-axis 48